COINS, CURRENCIES, SOCIAL CURRENCIES AND CRYPTOCURRENCIES

BRITANNIA 2021 1oz 999 FINE SILVER
GHANA · FREEDOM AND JUSTICE ·
UN PESO
PROVINCIAS DEL RIO DE LA PLATA
1813 - 2013
UNITED STATES OF AMERICA
E PLURIBVS UNVM
QUARTER DOLLAR
BITCOIN DIGITAL DECENTRALIZED PEER TO PEER
MONETARY METALS
1TROYOZ 999 FINE COPPER MJB

LEOPOLDO BEBCHUK

Coins, Currencies, Social Currencies, and Cryptocurrencies

Coins, Currencies, Social Currencies, and Cryptocurrencies

A Study on Monetary Instruments, Their Diversity, and Their Relationship with Credit-money

© Bebchuk, Leopoldo 2025

Coin, Currencies, Social Currencies, and Cryptocurrencies: A study about monetary instruments, their diversity, and their relationship with credit-money. 1st English edition

DOI: 10.13140/RG.2.2.36054.32328

ISBN: 978-631-00-9715-2

Original Title: *Monedas, Monedas Corrientes, Monedas Sociales y Criptomonedas: Un estudio acerca de los instrumentos monetarios, su diversidad y su relación con el dinero-crédito.*

DOI: 10.13140/RG.2.2.32789.40166

ISBN: 9-78-9878-89320-4

Buenos Aires, 2023

leopoldobebchuk@filo.uba.ar

This book was written as a final thesis for the Anthropological Sciences degree at the Faculty of Philosophy and Letters, University of Buenos Aires, and approved on May 6, 2022, as stated in the minutes COPDI-2022-03193139-UBA-DAADE_23FFYL

No reproduction in whole or in part of this work by any means whatsoever shall be punishable by any penalty.

If you would like to collaborate with its author, you can do so at the following Bitcoin address:

bc1qle0p0ldhg05savtwdvg9ueaj2w3qzcejhh6snf

Contents

Acknowledgments . . . . . **ix**
Preface . . . . . **xi**
Preface to the English version . . . . . **xv**
Preface to the printed Spanish edition . . . . . **xvii**
Preface to the printed English edition . . . . . **xxi**
Introduction . . . . . **xxiii**
1 Studies about Money **1**
Aristotle **3**
Theory I: The Metallic Paradigm **5**
1776–1850 Classical Economics 7
1867 Historical Materialism 8
1864 Genealogists 10
1875 Characterization 12
1905 Chartalism 14
1874-1920 Money and Credit 16
1890 Austrian School: Logical Origin and Typology 19
Observation: Ethnographical, Ethnological, Anthropological, and Ethological Approaches **27**
On the Antiquity of Currency. Trading with Monkeys 29
1875 Jevons: An Early Ethnology 35
1914-1924 Marcel Mauss: First Comprehensive and General Approach to Currency 37
1924 Armstrong: Shell Credit System 45
1949-1966 Einzig: Exhaustive Compendium of Ethnographies on Money 47
1944-1945 Primo Levi: Auschwitz Prisoners' Economy 55
1969 Godelier: Production and Circulation of Salt Currency . . . 62

Experimentation: Social Currencies **67**
Classification Schemes 70
The Red Global de Trueque (Endogenist, Issuance as Credit) . . 73
Red Mar y Sierra (Fiat Chartal) 79
Venado Tuerto (Chartal Shrinking) 82
Poriajhú (Debt Endogenist) 83
Cosettini Timebank (Tax Endogenist) 85
The Enemies of Social Currency 87
Theory II: New Paradigms **91**
General Theory of Credit and Money 93
Quantum Theory of Money 105
2 Money and Cryptography **111**
Bitcoin **113**
Origin 119
Value 127
Properties 156
Functions 165
Monetary Policy 186
Altcoins **193**
Privacy-focused Coins (Privacycoins) 195
Proof of Stake 198
Ethereum and Smart Contracts 200
Stablecoins 203
Social Cryptocurrencies 206
3 Final thoughts and conclusion **213**
Conclusion on the Taxonomy of Monetary Instruments . . **215**
The Philosophy of Cryptographic Money **219**
Economic (and Political) 221
A Social Theory of Cryptocurrencies 223
Money and Civilization 224
Change from Legal Tender to Cryptocurrency 226
The Future of Cryptocurrency 228
Sources **231**

To all those cypherpunks who fight against injustice and corruption every day of their lives.

Acknowledgments

First of all, I would like to thank my classmates throughout my university course, who helped me study, and the teachers who taught and evaluated me. To my classmates, Guadalupe Colque, Sofía Quevedo, and my *"Anthropo-team:"* Tomás Paya, Rocío Santarcieri, Sofía Laria, and Natasha Zamorano. Especially to my girlfriend, Lavinia Laviosa, for reviewing this work and helping me correct the last details before presenting it in its final form.

Secondly, I thank my tutors, Jorge Miceli and María Belén López Castro, especially the latter, who helped me shape this project. María helped me beyond her role as a tutor by giving me materials I was unaware of, which enriched this work.

Thirdly, I want to thank my thesis advisors, Juan Engelman and Sebastián Valverde, for their interest in and support of this research.

Fourthly, I thank Library Genesis and Sci-Hub for their unrestricted access to academic material. Without such initiatives, none of this would be possible. Their work is fundamental to the progress of all sciences.

Finally, thank you to Satoshi Nakamoto, whoever he is, for inventing Bitcoin. You gave me not just something to write about but a lot to also think about.

Preface

I can say that I learned about Bitcoin almost from its humble origins, although I overlooked its relevance for a long time. I first heard of Bitcoin in high school in 2010. I was fifteen years old and had built a desktop computer with a Pentium 4 processor, an upgrade from the one I had before. A friend of mine, Bonch, whom I called by his last name and because it sounded funny, was a very peculiar character. (I was, too. I still am, but at that time even more so.) He was always into weird things. One day, he told me that there was a secret internet that could only be accessed with a special browser called TOR, which was full of dark, illegal, bizarre, macabre, and even dangerous things. At that time, it was called the Deep Web, but today, it is known as the Dark Net.

I, of course, listened to him and went into the Deep Web to see what it was all about. It appealed to me because I had already spent the previous three years totally obsessed with antivirus, antispyware, firewalls, etc. I felt invulnerable in terms of computer security. Other friends did not dare to enter because many myths were circulating about that on the Internet: if you entered those sites, you would get viruses, hackers, curses, really anything was possible. Anyway, I went in and saw what kinds of things were there (and no, nothing happened to me).

At first, I noticed the terribly slow internet (my connection was already slow, but this was like going back to dial-up), no search engines, and old HTML sites — everything looked like an old version of the internet, like it had been before, in the 1990s. There were all kinds of fancy sites: pages to buy drugs, weapons, stolen stuff, child pornography, hitmen services, occultism, old software downloads; books about anarchy, black magic, and cryptography; underground news sites, corruption and political intrigues mixed with conspiracy theories, blogs of depressed people, hacker forums, sale of forged documents, tutorials to clone credit cards, etcetera, etcetera. And the word “Bitcoin” came up repeatedly when payments were involved.

My friend had told me something about Bitcoin, but I did not know much about it. We only understood that people used it to make payments on the Deep Web. I read on my own what it was, but the information

was scarce; all the articles said almost the same thing: that the Deep Web was a den of hackers, terrorists, and criminals, a cyberpunk world apart in which people paid with it. Nobody explained where it came from, how it worked, and what it was for, other than to pay without giving personal data (something logical if you were buying a lot of illegal stuff on shady Dark Net sites). So, I didn't even know where to get it; it just seemed to me that I would have to buy it with something, and I didn't have any money, so I didn't care too much. I also did not understand why there were so many books about cryptography, if it was such a technical, complicated, boring, and impractical subject. I didn't know whether it had something to do with the esoteric or what else (the word cryptocurrency didn't even exist; it was just Bitcoin).

It was not until four years later that the Bitcoin issue reappeared with some relevance in my life. I do not remember exactly when, but I think it must have been around 2014 at a family dinner. My grandfather (who passed away just as I was about to publish this work) asked about it, and my brother and I tried to answer him. We already knew the technical aspects by that time: that it is a big registry hosted in a peer-to-peer (P2P) network, that the transactions are solved by miners making the CPUs work, that the security was guaranteed by that CPU work, the P2P network, and the system of public and private keys, and that this all was to ensure anonymity. Still, he asked us more questions. "Why is it valuable?" We just did not understand that. My brother, for example, thought that the creator had made an enormous bank deposit to back Bitcoin. On another similar occasion, the subject came up again. Yet, at that time, we already knew that there was no such backing but rather that Bitcoin's worth was 'by itself.' Then, our grandfather became more incisive, asking, "Who takes responsibility in case of fraud?" "How can it work if no government backs it?" He became more moralistic and continued, "If I move money with it from one country to another, the economy minister (or the secretary of commerce, I don't remember exactly) would have a terrible problem?" We answered that no, because you would be moving neither pesos nor dollars, but the question of its social influence was still in my head.

Guided by this concern, I started looking for studies that said something about the social impact that Bitcoin could have. There was not much, but I found a blog with several essays specifically addressing that. There

were several short essays arranged in three main topics, as if they were volumes and chapters: (1) History and philosophy; (2) Economics; and (3) Politics. I read these and understood the relationship of everything I had seen and read before: Bitcoin was money created by cryptographic technology and was politically oriented. Behind that technical development, there was a political movement that planned to evade all governmental and institutional control by encrypting communications. Bitcoin was not money for buying illegal things on the Dark Net. Instead, Bitcoin, the Dark Net, TOR, and many other technologies were part of the efforts of freedom-minded people to create a society without the possibility of centralized control.

Understanding that potential, I got really involved with Bitcoin, learning how to use the software, buying some, reading the news, and telling everyone I knew about it. At the same time, I was already halfway through my anthropology degree, which had little to do with software, information and communication technology development and cryptography, but a lot to do with stateless and self-regulated societies. In 2015, I took an economic anthropology class and began to shape this work from there. I learned how economies operate where there is no government. Towards the end of the program, there were texts about the barter markets that emerged in the 2001 crisis in Argentina when the national currency was destroyed, so to speak. (I had not understood the magnitude of this when I lived through it, because I was barely six years old.) The blog I had read mentioned that Bitcoin would be valuable in weak economies and a crisis. It mentioned Argentina several times, and I also assumed that everything I had seen in TOR years before (those underground businesses) were just a first phase of Bitcoin's development. The second one would involve a gray area of the economy: products that, while not illegal, circulate unregulated. This is precisely what I understood barter markets to be: when the state-organized economy fails, local economies spontaneously emerge, and Bitcoin can benefit them. So, I started to save books, articles, and any information that had to do with all this, in a piecemeal way. Now that I have finished my degree, it is time to put all that to work.

Initially, this thesis was intended to have three parts: research that would bring me up to date with theories about currency, an introduction to Bitcoin and cryptocurrencies through a theoretical framework, and fieldwork to test the theoretical assumptions elaborated on. The year was

2020, and fieldwork had become impossible; moreover, there was not sufficiently well-established theoretical research to summarize in a few short paragraphs. I had to put aside that fieldwork and dedicate myself exclusively to developing a suitable theoretical framework to use in the future. Therefore, my work took a slightly different form than expected, but no less interesting.

Writing about events happening at the same moment is neither common nor easy. This topic is developing at an amazingly fast pace. Many of the things that seemed relevant at the time of writing are not so relevant now, and many unexpected developments have changed the landscape in various fields: technical, legal, and economic. Particularly China, which concentrated the greatest mining power within its borders, did away with the entire industry, leaving those miners to migrate to other latitudes. In Latin America, contrary to what was seen at the time of writing this study, an enormous opening to the circulation of Bitcoin began to take place. El Salvador passed a law to make it legal tender, while currently, Paraguay is developing a regulatory framework to promote the industry, and Argentina is beginning to debate a law that will allow salaries to be paid in Bitcoin. By the time you read this, these things may have also changed. However, I believe that despite this possible outdatedness concerning concrete events, some reflections and findings of this paper will be relevant despite such abrupt changes.

Leopoldo Bebchuk. Buenos Aires, 25th July 2021

Preface to the English version

The Spanish version's publication took much more time than I expected. As evidenced by the date at the end of the previous chapter, the work was finished by July 2021, but it wasn't approved until May 2022, almost a year later. There were at least three factors involved in that delay: bureaucracy in the university is awfully slow, the pandemic slowed it even more, and my research topic was so fringe that it was hard to gather an appropriate jury to evaluate it. Money and currency are not topics that are discussed very often. As my advisor said in my thesis defense, "Currency is a subject that has been little or not at all addressed in economic anthropology, which focuses on markets and other types of dynamics." On top of that, Bitcoin is such a new development that academic research has not caught up with it yet. It is not usual, nor easy, for a student to graduate by opening a new area of study, as there are no already-established authorities on the subject to rely on. Nonetheless, I did my best to accomplish that goal, and the university approved my work with one of the highest grades.

I have been planning to make an English translation of this work since the beginning, as I know that it will reach a higher audience and hopefully allow my findings to enter a broader debate. I waited for the university to approve the Spanish version before publishing it. Only after it was published did I start working on the English one, in case there were any corrections to make. It is more than a simple or literal translation; I modified more than just the main body text. In the original text, I tried to gather as many Spanish bibliographical sources as I could and translated the quotes from the ones that were unavailable. One of the merits I found in my work was to bring previously unavailable authors and ideas to the Spanish language version. In this English edition, I changed my sources to their English versions to make them easily accessible to the anglophone reader. It would be redundant to incorporate the extensive quotes that had been translated into Spanish.

Leopoldo Bebchuk. Buenos Aires, June 2022

Preface to the printed Spanish edition

It has been barely a year since this work was approved by the University of Buenos Aires and could finally begin to circulate over the Internet. However, many things have happened since then.

First of all, as soon as the thesis was approved and published in Spanish, I started working on the English edition, a process during which I made several corrections to the first Spanish version. It did not seem pertinent to me to add a new preface. Both versions were published completely openly and for free on the Internet, and I believe that they have had a good reception. But not everyone has the disposition to read a whole book from a screen, so I decided to create a print edition. This edition is a debt I had outstanding from the beginning.

Secondly, my academic career and my working career, which I had kept separate in my student years, were suddenly intertwined very tightly by a twist of fate, so to speak. In 2022, I had set three goals for myself: to graduate, to change jobs, and to have eye surgery. Leaving aside the third one, which I still haven't achieved to this day, I achieved the rest almost simultaneously between April and May of that year.

My thesis was really ready as early as 2021, after two years of work during the COVID-19 pandemic, but given the novelty of the topic and the slowness of the university bureaucracy, I only had a date for the final defense in May 2022. A month before that, at a birthday party with my lifelong friends (except the one who first told me about Bitcoin, with whom we lost contact), I told them that I was looking for a new job. With these friends, I shared several chat groups, one of which they had created especially for me to teach them about Bitcoin, blockchain and cryptocurrencies. In that conversation, one of them, Seba, had commented that the company he worked for was buying bitcoins at the drop of a hat, but he hadn't said the name or what he did.

After that party, Seba wrote to me and asked me if I wanted him to refer me to his work. I was just in the middle of an interview, and I told him not yet, because I might get hired at that company. After a few weeks in which I didn't hear back from that company, I told Seba that we can try getting me into his company. He sent me the link, and I was not a little surprised to see that the company was MicroStrategy, the largest Bitcoin holding company in the world. I immediately got the feeling that what I thought was going to be just a job to support me while I used my time for something more interesting (like writing about Bitcoin) was actually going to be a great opportunity.

I filled out the application, took four preliminary exams, three interviews, and was hired to be part of the technical support team, for which I was first going to have to take a five-week course along with other entrants. On my second day as an employee and still not knowing anything about my position or what the company does, there was an office-wide meeting with some important executives from my area who had come all the way from the United States. They were presenting throughout the morning, and at noon, there was a break where they greeted and met each new employee. I introduced myself in the most honest way I could find: "Today is my second day, I'm in support, I'm studying anthropology and I'm about to graduate with a thesis on Bitcoin." They seemed quite interested and said something about a Lightning node might help in the future. At the time, I didn't know what they meant, but today, there is already a Lightning product available. From there, I was known in the company as someone who had written a book about Bitcoin.

At the end of May, I was already finishing the bootcamp or entry course, and I met Luis, who manages the sales area in Latin America. I told him that I had just finished my career and about this job, which interested him a lot, and he is the one who later decided to make the company sponsor this print edition.

In August, MicroStrategy held an event for customers called MicroWorld LATAM, which is held every year and in which they give presentations on the product and new developments. I was asked to give a presentation on Bitcoin. Of course, I accepted. I gave it, and it was very well received, both within the company and by customers.

In November, LABITCONF, the biggest Latin American Bitcoin conference, was held in Buenos Aires, and the company participated. I asked

to go, since it is an activity carried out by the sales and marketing areas, of which I am not a part, and they allowed me to go. As a company, we had the highest level of access and a stand at the expo. During those days, I met ecosystem leaders from around the world, such as Obi Nwosu, Jimmy Song, and Elizabeth Stark. I was even able to meet the RSK and Money on Chain team and tell them about this very work, in which I wrote about their technologies. Alvaro D. Maria, author of *The Philosophy of Bitcoin* also came to our booth and gave me an unpublished copy of his book (in English) which he wanted to give to Michael Saylor, the co-founder and chairman of MicroStrategy. I agreed and, although it took time, we found a way to get it to him. I also had the opportunity to meet several media and industry companies.

In early 2023, MicroStrategy announced to all of its employees that it was going to start testing a Lightning rewards program internally. In the second quarter of the year, it announced that product publicly at MicroStrategy World 2023, which not only had a Bitcoin section but also a Lightning section. I, of course, followed everything very closely. During that time, I was asked to give two talks to explain what Lightning is to the rest of the Latin American employees, to which I obviously also agreed.

Also, by the vagaries of life, on another birthday, this time of a friend from college, I found out about Petricor, the publisher with whom I was able to bring the Spanish print edition to fruition.

I could not be more grateful to Seba for bringing me to MicroStrategy, to MicroStrategy in general for the opportunities it is giving me, and especially to Carolina Eliçabe Urriol and Luis Lombardi, for supporting me in all initiatives related to Bitcoin. Finally, with Julian Contreras and his publisher Petricor, for the excellent work on the Spanish printed version of the book.

The most significant addition to this edition is a small extra chapter after "Gresham's Law" about "Thiers' Law", a similar but inverse process proposed by Peter Bernholz, which I was not aware of before but found indispensable to add as soon as I learned of it.

A small caveat, or apology, if you will: the Einzig book used in my bibliography is actually not unique of its kind. There is another author who did very similar work and published it in the same year, 1949. *A Survey of Primitive Money; the Beginning of Currency*, by Alison Hingston Quiggin, was overlooked in my bibliography but would have greatly enriched this

work had it been included. I am also aware of a work by Wilhelm Gerloff entitled *Die Entstehung des Geldes und die Anfänge des Geldwesens* (The Origin of Money and the Beginnings of the Monetary System), which is only available in German, making it more difficult for me to access. Also, I am currently reading *Debt: The First 5000 Years* by David Graeber, another book that I would also have liked to include in the bibliography of this work. I did not want to fail to mention them, since one of the objectives of this work is to present an updated state of the art.

Leopoldo Bebchuk. Buenos Aires, May 2023.

Preface to the printed English edition

Two years have passed since I published the Spanish printed version in 2023, and it is with great pleasure that I am now working on the English printed and corrected version I was also longing to make available.

In the course of these two years at MicroStrategy, now Strategy, I was promoted not just to participate in LABITCONF as part of our booth, but also as a speaker, representing the company in front of the Latin American public, twice. I was also promoted to work in the Lightning Rewards and a new project called Orange Check as Product Manager, two Bitcoin products the company wanted to release to promote Bitcoin adoption among enterprises beyond treasuries.

Unfortunately, both projects were subsequently cancelled, and I moved back to work on Strategy's business intelligence platform in my new Product Manager role. The company continued its path in Bitcoin treasuries and refined it to higher levels since then. Both last year and this year, I participated in our Strategy World, first presenting our Bitcoin products, then as part of our business intelligence platform.

In the meantime, I was also invited to work as an author providing opinion pieces to Criptonoticias, the leading Latin American digital media on Bitcoin, blockchain and cryptocurrencies. I have used several of their pieces in this very work, so it is a great honor to now be part of the media as well.

By the time I started working at Strategy and this book was first released, I submitted an abstract of a paper to a project called The Satoshi Papers, led by fellow anthropologist Natalie Smolenski, the Texas Bitcoin Foundation, and the Bitcoin Policy Institute. It was also this year that the book was finally published, so this English reviewed edition of *Coins, Currencies, Social Currencies, and Cryptocurrencies* cannot come at a better time. I am deeply grateful to the Konsensus Network team that has worked so hard on making this edition possible.

Leopoldo Bebchuk. Buenos Aires, June 2025

Introduction

> "En la calle Belgrano tomé un taxímetro. Insomne, poseído, casi feliz, pensé que nada hay menos material que el dinero, ya que cualquier moneda (una moneda de veinte centavos, digamos) es, en rigor, un repertorio de futuros posibles. El dinero es abstracto, repetí, el dinero es tiempo futuro. Puede ser una tarde en las afueras, puede ser música de Brahms, puede ser mapas, puede ser ajedrez, puede ser café, puede ser las palabras de Epicteto, que enseñan el desprecio del oro; es un Proteo más versátil que el de la isla de Pharos. Es tiempo imprevisible, tiempo de Bergson, no duro tiempo del islam o del Pórtico."
>
> — Jorge Luis Borges, "El Zahir"[1]

> "Remember that Time is Money. He that can earn Ten Shillings a Day by his Labour, and goes abroad, or sits idle one half of that Day, tho' he spends but Sixpence during his Diversion or Idleness, ought not to reckon That the only Expence; he has really spent or rather thrown away Five Shillings besides.
> Remember that Credit is Money. If a Man lets his Money lie in my Hands after it is due, he gives me the Interest, or so much as I can make of it during that Time. This amounts to a considerable Sum where a Man has good and large Credit, and makes good Use of it."
>
> — Benjamin Franklin, "Advice to a Young Tradesman"[2].

Cryptocurrencies, with more than ten years of existence, are no longer a phenomenon that we could call novel. However, it is still largely unexplored by the social sciences and the humanities. Some work has been done in this regard, most notably the book *The Bitcoin Standard* by Saifedean Ammous.[3] It situates the phenomenon in monetary history and proposes

[1] Jorge Luis Borges, "El Zahir," in El Aleph (Editorial Losada, 1949), 105.

[2] Benjamin Franklin, "Advice to a Young Tradesman," 21 July 1748, in The Papers of Benjamin Franklin, ed. Leonard W. Labaree, vol. 3 (Yale University Press, 1961), 304–308, Founders Online, National Archives, https://founders.archives.gov/documents/Franklin/01-03-02-0130

[3] Saifedean Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking* (Wiley, 2018).

its subsequent development based on the Austrian school of economics theories. However, this book is more oriented to dissemination than to academic discussion. In this field, we can find the thesis of Peyrouzet García Siñeriz *In Blockchain They Trust*[4] and Mark Alizart´s *Cryptocommunism*[5], of a political and philosophical nature. On the other hand, Argentina has had significant intellectual development in cryptocurrencies. From a citizen having registered the "bitcoins" internet domain eight years before its creation[6] and the formation of an NGO and pioneering buying and selling platforms in the region[7] to the development of innovative projects such as RSK.[8] It is, then, the first objective of this thesis to introduce Bitcoin, cryptocurrencies, and blockchains in the social sciences, from an anthropological and economic perspective, without neglecting their mathematical and technical foundations.

Secondly, this work studies cryptocurrencies, among others, as one form of currency. However, to carry out such an undertaking, it was necessary to address history, if not money itself, then studies about it. Money and currency are rather marginal objects of study in both anthropology and economics, a point to which I will return throughout this text. Those familiar with the most important authors and schools in anthropology will notice the almost total absence of any mention of them in this study. That is why the entire first part is not devoted to cryptocurrencies but to currencies in general and the theories about them, both in economics and anthropology. This work is, therefore, a study of money and currencies in general, including cryptocurrencies.

It is worth clarifying two of the grammatical conventions used in this paper. The first is a standard convention in the literature related to the subject and is noted in several books: it is the difference between "bitcoin" (common noun) and "Bitcoin" (proper noun). Bitcoin refers to the entire payment system, while bitcoin or bitcoins are the currencies circulating

[4]Mateo Peyrouzet García-Siñeriz, "In Blockchain They Trust – Now, Power to the People or to the invisible Hand? An Analysis of the Ideological Tensions and Affinities Between Crypto-libertarian and Crypto-commonist Visions, Projects and Aspirations for the Blockchain Revolution" (Diss., University of Exeter, 2018).

[5]Mark Alizart, *Cryptocommunism (Theory Redux).* (Polity Press, 2020). https://libgen.rs/book/index.php?md5=A666241D7F49D33F423E5AE1776D19EA.

[6]Nicolás Antiporovich, "Rodolfo Andragnes, el Argentino que Registró el Dominio Bitcoins.com en el Año 2000," *CriptoNoticias - Bitcoin Blockchains Criptomonedas* (2020).

[7]"Quienes Somos," ONG Bitcoin Argentina, accessed 31 August 2020, https://www.bitcoinargentina.org/quienes-somos/.

[8]Sergio Demian Lerner, "Rsk.," *Rootstock Core Team, White Paper*, (2019).

within it. The second clarification is why go against another convention concerning the gender of the common noun "bitcoin." The English reader may skip the second as it regards a purely Spanish matter. The Spanish-speaking community tends to speak of bitcoins in the masculine form: "*los bitcoins,*" but I consider this incorrect for the following reasons. The word "bitcoin" is a compound: "bit" (minimum unit of information, in turn a condensation of binary digit) and "coin" (currency). However, bit, which is a masculine noun, is not the nucleus but a modifier, an adjective; coin, " which is feminine, is the noun. This is even more striking when one observes that Spanish speakers have no problem choosing the noun altcoins, which have the same structure as the feminine. I suspect this convention has something to do with automatic translations made in the early days of Bitcoin and used a generic masculine article or the Iberian custom of treating Anglicism as masculine (e.g., "el internet"). To a lesser degree, this also happens with the term "blockchain," which is not uncommon to find in masculine, but is usually used in feminine. Throughout this paper, I will use "bitcoin" as a feminine common noun and as plural "*las bitcoins*" and not "*los bitcoines*".

This work is divided into three parts. The first part is divided into three sections: a theoretical section (divided into two parts), an empirical section, and an experimental section. The theoretical section lists and briefly explains the theories about money and currency, or what place these elements occupy in more general economic theories. The empirical section gathers specific cases of monetary systems documented mainly, but not exclusively, by ethnographers. The experimental section is devoted to the phenomenon of social and complementary currencies, which are monetary systems purposely made by their users; unlike the cases in the previous section, whose origins are largely unknown.

The second part is devoted to Bitcoin in particular and cryptocurrencies in general, and it is also divided into three sections. The first section deals with Bitcoin and is subdivided into subsections, three of which are individual chapters. The first chapter deals with the creation of Bitcoin in a technical and political sense, to put its emergence in context. The following subsection, on value, consists of four chapters that put Bitcoin under the magnifying glass of different theories of value. The following subsection explains the characteristics of Bitcoin and how they equate to the physical properties that a material must have to function as currency.

This subsection is based on Jevons's postulates,[9] introduced in the first part and widely accepted in economic science. The following section analyzes to what extent Bitcoin fulfills the functions assigned to money by economic science, in the same way that Paul Einzig studied them for what he calls "primitive money."[10] The last subsection, also a single chapter, explains Bitcoin's monetary policy and how it works. The second section of part two consists of five chapters on cryptocurrencies other than Bitcoin. Finally, the third part contains the final thoughts and conclusions.

This work's most important bibliographical source is *Primitive Money in Its Ethnological, Historical and Economic Aspects* by Paul Einzig, mentioned in the previous paragraph.[11] From that monumental work, I obtained most of the ethnographic examples cited in the first part and the analysis scheme developed in the second part. On the theoretical side, Mostafa Moini's work, "*Toward a General Theory of Credit and Money,*" explained in detail in a chapter of the first part, has been of profound influence and much use to me in developing this thesis.[12] In fact, it is thanks to Moini's mention that I discovered Einzig's work. Until then, finding ethnographies on monetary systems had been exceedingly difficult. As for bibliography about Bitcoin, the most complete work is *Mastering Bitcoin* by Andreas Antonopoulos.[13]

Regarding translations, I have tried to cite the bibliography and sources in English if available, but some sources do not exist in this language. All quotations, however, are in English, taken from original sources unless noted in the reference. In the case of Satoshi Nakamoto's correspondence, it can be found entirely in Phil Champagne's *The Book of Satoshi*.[14] Still, I quoted the sources directly from the Nakamoto Institute because I did not like the way they were translated into Spanish in that book when I wrote the original text. Journalistic sources had been left as they were in the original Spanish version.

[9]William Stanley Jevons, *Money and the Mechanism of Exchange*, (D. Appleton and Company, 1877), 31.

[10]Paul Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects* (Eyre & Spottiswoode 1966), 428.

[11]Ibid., 7.

[12]Mostafa Moini, "Toward a General Theory of Credit and Money," *Rev. Austrian Econ.* 14 (2001): 267–317.

[13]Andreas Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, (O'Reilly Media, 2017).

[14]Phil Champagne, *The Book of Satoshi* (e53 Publishing, 2014).

Finally, this work tries not to delve too deeply into the technical aspects of Bitcoin or other cryptocurrencies since such studies abound. I am not an author suited to engage in such discussions either. However, it has been necessary to understand certain aspects of how cryptocurrencies work and their capabilities and limitations. I hope that does not pose a problem for the reading of this work.

Part 1

Studies about Money

Aristotle

… For people seek to return either evil for evil — otherwise they feel like slaves — or good for good — otherwise no exchange takes place, and it is exchange that holds them together. This is why they erect a temple of the Graces in a conspicuous place, so that benefits might be repaid. This is the special characteristic of grace, because one ought both to perform a return service to someone who has been gracious, and another time to make the first move by being gracious oneself.

It is a diagonal conjunction that produces proportionate reciprocation. (…) The builder must get from the shoemaker the product of his labour, and must hand over his own in return. If, first, proportionate equality is established, and then reciprocation takes place, the result we mentioned will follow. If not, there is no equality, and the bargain falls through, since there is no reason what one produces should not be more valuable than what the other produces, and the products must therefore be equated. (…) This is why everything that is exchanged must be in some way commensurable. This is where money comes in; it functions as a kind of mean, since it is a measure of everything, including, therefore, excess and deficiency. (…) Everything, then, must be measured by some one standard, as we said before. This standard is in fact demand, which holds everything together; for if people needed nothing, or needed things to different degrees, either there would be no exchange or it would not be the same as it now is. But by social convention money has come to serve as a representative of demand. And this is why money is called *nomisma*, because it exists not by nature but by convention (*nomos*), and it is in our power to change its value and to render it worthless. There will be reciprocity, then, when the equation has been made (…).

> Money is, as it were, our guarantor for future exchange: if we do not need a thing now, we can have it if ever we do need it, since we must be able to get it if we pay. The same thing happens to money as to other commodities, in that its value is not always the same, but it does tend to be more stable. Everything, then, must have a value put on it, because then there will always be exchange, and if exchange, association between people.[1]

In the fourth century B.C., Aristotle defined currency as a measure that equated all goods in circulation and as a guarantor of reciprocity between people. It is human-made instead of natural development, and moral rather than instrumental in nature. It is important to bring up his definition first, because it is one of the oldest and because of the influence of this author in the development of modern sciences. It will then be seen how much of his definition has shaped later ideas about money and how much has been overlooked or rediscovered much later.

[1]Aristotle, *Nicomachean Ethics* (Cambridge University Press, 2004), 89–91.

Theory I: The Metallic Paradigm

The first theoretical section explains the place given to money and currency by different schools of economics, from the first scientific formulations of the subject during the Enlightenment to the beginning of the twentieth century, when the debate on the subject was relegated to the background.

In chronological order, the first definition can be seen in Adam Smith, which was adopted by successive classical authors and later by Marxism without major criticisms. It was not until the end of the nineteenth and the beginning of the twentieth centuries that counter-explanations and debates began to appear, which did not last beyond the 1940s.

For this summary, I resorted directly to the original works of the cited authors rather than to texts about them by third parties. However, translations of some of them were used. Some comments on certain terms were necessary in these cases to avoid confusion.

◆ 1776–1850 Classical Economics

Most classical economists paid little attention to money. In his 1776 book, *An Inquiry into the Nature and Causes of the Wealth of Nations*, Adam Smith (1723-1790) only devoted Chapter 4 to the topic. Before arriving at a definition of money, it is necessary to examine the concept of value, which is fundamental to economics. Smith explicitly states in the *Wealth of Nations* what he sees as the concept of value:

> …The value of any commodity, therefore, to the person who possesses it, and who means not to use or consume it himself, but to exchange it for other commodities, is equal to the quantity of labour which it enables him to purchase or command. Labour, therefore, is the real measure of the exchangeable value of all commodities.[1]

This is subsequently known as *labor-value*. A second concept, derived from this, is that of *exchange-value*:

> …Every commodity, besides, is more frequently exchanged for, and thereby compared with, other commodities than with labour. It is more natural, therefore, to estimate its exchangeable value by the quantity of some other commodity than by that of the labour which it can purchase.[2]

Last, we have a third distinction and a different type of value:

> The word value, it is to be observed, has two different meanings, and sometimes expresses the utility of some particular object, and sometimes the power of purchasing other goods which the possession of that object conveys. The one may be called "value in use"; the other, "value in exchange." The things which have the greatest value in use have frequently little or no value in exchange; and, on the contrary, those which have the greatest value in exchange have frequently little or no value in use. Nothing is more useful than water: but it will purchase scarce anything; scarce anything can be had in exchange for it. A diamond, on the contrary, has scarcely any value in use; but a very great quantity of other goods may frequently be had in exchange for it.[3]

[1] Adam Smith, *An Inquiry Into the Nature and Causes of the Wealth of Nations* (University of Chicago Press, 1977), 50.
[2] Ibid., 52.
[3] Ibid., 48.

As for money, he understands it as a commodity that mediates exchanges to avoid an inconvenience in direct exchange:

> One man, we shall suppose, has more of a certain commodity than he himself has occasion for, while another has less. The former consequently would be glad to dispose of, and the latter to purchase, a part of this superfluity. But if this latter should chance to have nothing that the former stands in need of, no exchange can be made between them. (…)
>
> In order to avoid the inconveniency of such situations, every prudent man in every period of society, after the first establishment of the division of labour, must naturally have endeavoured to manage his affairs in such a manner as to have at all times by him, besides the peculiar produce of his own industry, a certain quantity of some one commodity or other, such as he imagined few people would be likely to refuse in exchange for the produce of their industry.[4]

Smith mentions that various commodities may have occupied that place, gives some historical contemporaneous examples, and then states that metals have become preferred. This is followed by a history of the different currencies and the weights and measures that give them their name. He then explains the value of commodities by leaving aside money only as a measure for the value of other commodities.

The rest of the classical authors are satisfied with this definition and therefore do not devote much attention to this subject.

◆ 1867 Historical Materialism

Almost a century later, Karl Marx (1818-1883) does likewise. He devotes Chapter 3 of the first volume of *Das Kapital. Kritik der Politischen Ökonomie [Capital. A Critique of Political Economy]* (1867), to money.[5] He argues:

> …The particular commodity, with whose bodily form the equivalent form is thus socially identified, now becomes the money commodity, or serves as money. It becomes the special social function of that commodity, and consequently its social monopoly, to play within the world of commodities the part of the universal equivalent.[6]

[4] Ibid., 42.
[5] Karl Marx, *Capital: A Critique of Political Economy*, Volume One. (1867).
[6] Ibid., 46.

> …money itself has no price. In order to put it on an equal footing with all other commodities in this respect, we should be obliged to equate it to itself as its own equivalent. (…) although the money that performs the functions of a measure of value is only ideal money, price depends entirely upon the actual substance that is money. The value, or in other words, the quantity of human labour contained in a ton of iron, is expressed in imagination by such a quantity of the money-commodity as contains the same amount of labour as the iron.[7]
>
> The price-form, however, is not only compatible with the possibility of a quantitative incongruity between magnitude of value and price, i.e., between the former and its expression in money, but it may also conceal a qualitative inconsistency, so much so, that, although money is nothing but the value-form of commodities, price ceases altogether to express value.[8]

Neither Smith nor Marx (and, consequently, neither the schools they founded with their thought) was interested in studying money itself, or as something significant. Rather, they focused on the function it fulfills in an economic system. That is why they devote only one chapter to it; they consider that the function of money is carried out only by gold and silver, and they do not problematize its nature. They consider it to be something given and not worthy of further reflection. Karl Marx, as seen in the paragraph quoted above, finds an incongruence between labor value and the currency's exchange value. However, he is still far from seeing that the use-value of the currency as a medium of exchange contributes some extra exchange value. This is not surprising given Marx's reliance on the labor-value theory. The theory of value that focuses on use-value had not yet arrived, but it is important to note that this problem was already present in these theories. The Austrian school will pay special interest to currency and the circular relationship between its exchange value and its use value as a medium of exchange.

On the other hand, Marx developed a powerful concept that can explain a different problem that will appear repeatedly in this study. This he called fetishism and presents it in this way:

> A commodity is therefore a mysterious thing, simply because in it the social character of men's labour appears to them as an objective

[7] Ibid., 67.
[8] Ibid., 70.

> character stamped upon the product of that labour; because the relation of the producers to the sum total of their own labour is presented to them as a social relation, existing not between themselves, but between the products of their labour. (…) There it is a definite social relation between men, that assumes, in their eyes, the fantastic form of a relation between things. In order, therefore, to find an analogy, we must have recourse to the mist-enveloped regions of the religious world. In that world the productions of the human brain appear as independent beings endowed with life, and entering into relation both with one another and the human race. (…) This I call the Fetishism…[9]

For him, money plays a vital role in this concealment:

> It is, however, just this ultimate money form of the world of commodities that actually conceals, instead of disclosing, the social character of private labour, and the social relations between the individual producers.[10]

Despite having elucidated such a powerful concept, he also fell into fetishism in his treatment of money, as I explain later.

◆ 1864 Genealogists

During the second half of the 19th century, influenced by Charles Darwin's and Wallace's foundational work, *On the Origin of the Species by Means of Natural Selection, or Preservation of Favored Races in the Struggle for Life* (1859), social scientists adopted conceptual schemes from biology, just as the physiocrats had used biological metaphors to explain political economy.[11] This manifested itself, broadly speaking, in two ways: the first, in separating the evolutionary process into phases or stages; the second, in establishing a genealogical taxonomy and searching for the origin of a given social phenomenon. The second tendency is the most novel, given that Darwin's great discovery was to note that the fossil species found were in some way related to present-day species. An evolutionary history could be traced by following their changes. On the other hand, the first tendency

[9] Ibid., 47–48.
[10] Ibid., 50.
[11] Charles Darwin. *On the Origin of Species by Means of Natural Selection, or Preservation of Favored Races in the Struggle for Life*. (John Murray, 1859).

has antecedents as old as Hesiod and was present in the social sciences from their beginnings during the Enlightenment.[12] In the period referred to, however, we find a new upsurge of this conception. If we quickly review some exponents of this trend, we see historical materialism, with its idea of the modes of production,[13] particularly in Lewis Henry Morgan´s work from 1877,[14] and part of Durkheim's works.[15] This paradigm is known as unilinear evolutionism or unilinear cultural evolution, since it understands the evolution of human social organization as directed in one direction. It presupposes that cultures will go through certain stages during development. At this point, it departs from Darwin's and Alfred Russell Wallace's theory of evolution by natural selection, which does not have a univocal tendency for all cases.

Regarding the subject of this study, we find the work of Hildebrand (1812-1878) framed in this paradigm. Following the trend of unilinear evolutionism and an ancient custom among Germanic scholars of dividing history into three stages, this German economist, a contemporary of Morgan and a little later than Christian Jürgensen Thomsen,[16] presented the idea of an evolution of money in three stages.[17] First, there would be a barter economy (*Naturalwirtschaft*, natural economy), from which one passes to a mercantile economy (*Geldwirtschaft*, money economy), and finally one

[12]Hesiod, *Works and Days*. Translated by H.G. Evenlyn-White, (Harvard University Press, 1914).

[13]The modes of production (*Produktionsweise*) proposed by Marx and Engels are, in evolutionary order: primitive communism, slavery, feudalism, capitalism and modern communism or socialism. See Friedrich Engels, *The Origin of the Family, Private Property and the State* (2021); K. Marx, *A Contribution to the Critique of Political Economy* (1999), Preface.

[14]Lewis Henry Morgan, *Ancient Society or Researches in the Lines of Human Progress from Savagery through Barbarism to Civilization* (Calcuta 1982). This influential work laid the foundations of linear evolutionism in anthropology. It understands human progress as a universal development, although not simultaneous for all societies, in three major stages: savagery, barbarism and civilization, subdivided into three levels each: lower, middle and upper.

[15]Émile Durkheim, *The elementary forms of the religious life, a study in religious sociology* (London 1915); É. Durkheim, *The Division Of Labour In Society* (London 2017) In the latter (1893), he proposes the passage from a mechanical solidarity, typical of traditional societies, to an organic solidarity, typical of modern societies, with greater division and specialization of functions. In the former (1912), he isolates the basic elements of religion from what he considers its simplest documented forms.

[16]Christian Jürgensen Thomsen is the one who systematically periodized European prehistory in the three stages: stone, bronze and iron ages. Christian Jürgensen Thomsen, "A Brief Overview of Monuments and Antiquities from the Nordic Past," In *Guide to Northern Archaeology*. (Royal Society of Northern Antiquaries, 1836): 27-90.

[17]Bruno Hildebrand, "Naturalwirthschaft, Geldwirthschaft und Creditwirthschaft," 2 (1864): 1–24.

arrives at a credit economy (*Creditwirthschaft*). This work is little known; it was not even translated from German, but it has permeated economic science as an origin myth and unchallenged and untested common sense. Many subsequent economists, even contemporary ones, consider this simple explanation of the evolution of money to be perfectly valid and do not think there is anything more to say about it.

Contemporaneous with this hypothetical approach, the naturalist Robert E. C. Stearns documented the use of seashells as currency by various Aboriginal groups in the United States, Africa, and India.[18] One of his works, "Aboriginal Shell Money," although brief, contains a great deal of information regarding the species of shells used, how the beads used as money were made, and even the dollar values assigned to them. We can consider this author a precursor, since anthropology as a discipline only turned its attention to economics in the 1920s, as I will detail later.

◆ 1875 Characterization

William Stanley Jevons (1835-1882), economist and logician, is recognized as one of the founders of the marginalist school of economics, together with Leon Walras and Carl Menger, of whom I will speak later. But I am not so interested in the development of Jevons's theory as in his characterization of money, which, as happened with Hildebrandt and his theory's origin myth as it transcended until it became part of the economic zeitgeist, somewhat obfuscating its original conception.

Jevons develops these ideas in his 1875 work, *Money and the Mechanism of Exchange*.[19] Right from the beginning, the table of contents contains quite clear information about the issues addressed and the magnitude of this work. The first chapter pays homage to the genealogical tradition of which I spoke in the previous chapter and deals with barter and the supposed problems it brings with it: the coincidence of needs, which is defined as, "to find two persons whose disposable possessions mutually suit each other's wants;"[20] the measure of value, "each commodity would have to be quoted in terms of every other commodity, or else complicated

[18] Robert.E.C. Stearns, "Aboriginal Shell Money," *American Naturalist* 11, no. 6 (1877): 344–50.

[19] Jevons, *Money and the Mechanism of Exchange*, xi.

[20] Ibid., 3.

rule-of-three sums would be necessary;"[21] and subdivision, certain goods are not plausible to be fractionalized and "we need a means of dividing and distributing value according to our varying requirements."[22]

The second chapter deals with exchange, where Jevons defines "money as the measure and standard of value and the medium of exchange."[23] From that definition, he derives its functions:[24]

1. Medium of exchange
2. Measure of value
3. Standard of value[25]
4. Storage of value[26]

Chapter 4 deals with the early history of money, albeit as it is used in hunter-gatherer and pastoral societies. He uses biblical quotations, colonial documents, and etymological studies since ethnology had not yet been developed, which I will explain in the following section. He continues by mentioning personal ornaments and other manufactured items as currency.

Like the third chapter, the fifth chapter defines properties that are immensely important for economic theory. In order of importance, an object requires the following properties to function successfully as money:

1. Utility and value
2. Portability
3. Indestructibility
4. Homogeneity
5. Divisibility
6. Stability of value
7. Cognizability[27]

[21] Ibid., 5.
[22] Ibid., 6.
[23] Ibid., 8.
[24] Ibid., 13.
[25] Ibid., 14.
[26] Ibid., 15.
[27] Ibid., 31.

Subsequent chapters deal with different historical and technical aspects of currencies and banking systems, which are irrelevant to this part of the study but will be addressed later.

◆ 1905 Chartalism

Georg Friedrich Knapp (1842-1926) published his work *Staatliche Theorie des Geldes [The State Theory of Money]* in 1905.[28] It laid the theoretical foundations and coined the term "chartalism" from the Latin word "*charta*" [paper], thus founding one of the heterodox schools of economics. Knapp classified money according to its origin and function.

Table .1: Scheme of classification of means of payment according to their origins, taken from the English edition of 1924.[29]

<table>
<tr><th colspan="6">Means of payment are</th></tr>
<tr><th colspan="2">Pensatory</th><th colspan="4">Chartal, i.e., money</th></tr>
<tr><th>Amorphic</th><th>Morphic</th><th colspan="2">Hylogenic</th><th colspan="2">Autogenic</th></tr>
<tr><td rowspan="2">I
Autometallism
goes here</td><td rowspan="2">II Ducat
example (p. 28)
goes here</td><th>Orthotypic</th><th>Not orthotypic</th><th>Metallo-
plastic</th><th>Not metallo-
plastic</th></tr>
<tr><td>(1) III Money in kind</td><td>(2) IV</td><td>(3) V</td><td>(4) VI
Paper
money</td></tr>
</table>

The following quotations should clarify the terminology used in the scheme:

> Pensatory: "Pensatory practice, on the other hand, means the practice of weighing at the time of payment to establish the validity. Since there is such a thing as a wearing down of the pieces, it is necessary to keep the two distinct."[30]
>
> Morphic: "Morphism gives the possibility of recognising the means of payment without the necessity, which previously existed, of naming any given substance, for the legal ordinances describe the permissible pieces explicitly."[31]

[28] Georg Friedrich Knapp, *The State Theory of Money*, (Macmillan & Company, 1924).
[29] Ibid,. 70, 73.
[30] Ibid., 28.
[31] Ibid., 27, 28.

> Orthotypic: "We will call it orthotypic to indicate that the specific content of the pieces is dependent on that norm ("ortho"). So non-specie kinds of money might be called 'notal' or paratypic money, to show that it is counter to (para) that norm."[32]
>
> Hylogenic: If the law establishes that a particular metal can be physically converted into money without limit, it is a genetic relation between money and metal. We call this metal hyllic. The hylenic norm establishes how many units of money value will be produced from one unit of weight of the given metal. If this conversion is made with free coinage and the piece's content meets the standard, we will have money in metallic form. Everything else is notal, whether coins or banknotes, pure and simple.[33]

The main argument of the work and the chartalist school is that money originates in law. He defines money as follows: "Money always signifies a Chartal means of payment. Every Chartal means of payment we call money. The definition of money is therefore 'a Chartal means of payment.'"[34] And he defines a chartal medium in this way, "Perhaps the Latin word '*Charta*' can bear the sense of ticket or token, and we can form a new but intelligible adjective: 'Chartal.'" Our means of payment has this form of token, or Chartal, form."[35]

Knapp's main theoretical adversary is "metallism," which holds that money has a value according to the material from which it is made. "Validity by proclamation is commonly called the 'face value' in contrast with the 'intrinsic value' of the pieces, which is supposed to depend on their metallic content. This is a habit of metallists, who are always autometallists at heart."[36]

As for functional classification, he has a criterion according to the directionality of payments: (a) to the state (epicentric); (b) from the state (apocentric); (c) other payments (paracentric). In addition, he differentiates between current money, optional and small change; and between definitive money, *valuta*, and forms of provisional or accessory money legally convertible to the former.[37]

[32] Ibid., 66.
[33] Ibid., 60.
[34] Ibid., 38.
[35] Ibid., 32.
[36] Ibid., 30.
[37] Ibid., 12.

◆ 1874-1920 Money and Credit

Henry Dunning Macleod (1821-1902) was the first economist to propose a theory of credit, in an extensive work appropriately *The Theory of Credit.*[38] He is an economist who was not very well known at the time and remains unknown to this day. However, he will play a particularly significant role in a newer theory that I will discuss later, which is why I comment on him here.

In an earlier work, *The Elements of Banking*, Macleod makes the most forceful statement about money: "money and credit are homogeneous quantities, and that money is only the highest and most general form of credit."[39] In his theory of credit, he further elaborates this idea:

> [Money] is simply a right or title to demand some product or service from some one else.
>
> [A person] agrees to accept it in exchange for the services he has rendered, because he believes, or has confidence, that he can purchase some satisfaction which he does require, at any time he pleases. Money, is therefore, what is called credit (…).
>
> A whole series of writers from the earliest times have perceived that the true nature of money is merely a right or title to acquire a satisfaction from someone else, i.e., a credit (...).
>
> Now, that credit is as good as money will appear: it is to be observed that money itself is nothing but a kind of security which men receive upon parting with their commodities, as a ground of hope or assurance, that they shall be repaid in some other commodity: since no man would either sell or part with any for the best money, but in hopes thereby to procure some other commodity or necessary.[40]

Having established that, he could go no further, since not only did he not gain acceptance of his ideas by his colleagues, but he was, so to speak, on the fringes of marginalist theory and other progress that economists were making at that time. Thus, his theory remained disconnected from

[38] Henry Dunning Macleod, *The Theory of Credit* (Longmans, Green and Company, 1893): Pt. 1; Henry Dunning Macleod, *The Theory of Credit* (Longmans, Green and Company, 1894): Vol. 1, Pt.2: ; Henry Dunning Macleod, *The Theory of Credit* (Longmans, Green and Company, 1897): Vol. 2, Pt. 2.

[39] Henry Dunning Macleod, *The Elements of Banking* (Longmans, Green and Company, 1891), 21.

[40] Macleod, *Theory and Credit*, 75–76.

the prevailing paradigm, and credit continued to be considered rather as something derived from money than something from which money derives.

Leon Walras (1834-1910) is another economist who contributed to the development of marginalist theory in economics. Together with Jevons, mentioned above, and Menger, whom I will deal with later, they developed the theory of utility-value instead of the labor-value theory of classical political economy. Yet, his contributions to understanding money are the most important in this work. Two concepts he formulated in his *Éléments d'Économie Politique Pure ou Théorie de la Richesse Sociale* [*Elements of Pure Political Economy or Theory of Social Wealth*], published several times from 1874 until it reached its final form in 1926, are of interest. These concepts are the *numéraire* and the *étalon*.

> …the situation of a market in a state of general equilibrium can be completely defined by relating the values of all the commodities to the value of any particular one of them. That particular commodity is called the *numéraire* [or standard commodity], and a unit quantity of this commodity is called a standard [*étalon*].[41]

Hence, if the *numéraire* is, for example, salt, the *étalon* is a given quantity, for example, 100g. In modern terms, *numéraire* is translated as commodity of account or medium of exchange, and *étalon* as unit of account. With this postulate, Walras established that a unit of account is implicit in a price system that arises when several commodities are exchanged. From there, he goes on to describe money:

> In general, however, the commodity which serves as the *numéraire* serves also as money and acts as a medium of exchange. The standard of measure of value [*étalon numéraire*] thus becomes the monetary standard [*étalon monétaire*]. The two functions are, nevertheless, distinct, even when they are found in the same commodity.[42]

It is essential to clarify that these functions were repeatedly confused. The second part of the theory section will explain the importance of this separation, as although they are combined, they remain distinct.

For now, let us turn to another contemporary formulation: the pure credit system of Knut Wicksell (1851-1926) in his *Föreläsingar i national*

[41] Leon Walras, *Elements of Pure Economics or The Theory of Social Wealth* (George Allen and Unwin Ltd., 1965), 185.

[42] Leon Walras, Éléments d'économie politique pure ou Théorie de la richesse sociale (Lausanne 1874), 149.

ekonomi [*Lessons in Economics*], published around 1935, but probably written between 1900 and 1916.[43]

Although Wicksell understands credit as a derivative of money, rather than as money itself, he allowed himself the intellectual exercise of imagining a credit-only monetary system. He develops it in a long chapter entitled "The 'Ideal Bank' and the Obstacles to its Realization,"[44] after having presented it schematically in the previous chapter:

> If we suppose, for the sake of simplicity, that all such business is concentrated in a single bank with branches in all business centres throughout the country and that the keeping of a bank account has become universal (...), the position in the money market will be as follows. The whole monetary stock of the country will be collected in the vaults of the bank and will be, so far as internal turnover and business activity are considered, absolutely idle. All payments will be made by cheques drawn on the payer's banking account, but these cheques will never lead to any withdrawals of money from the bank, but only to a transfer to the payee's account in the books of the bank. On the other hand, the bank cannot lend in concreto a farthing of the money deposited with it, because it would flow back to the bank in the form of deposits as soon as it had been used.
>
> (...) payments will be made by successive drawings by the borrower upon his credit in the bank, and every such cheque must naturally lead to a credit with another person's (the seller's) account, either in the form of a deposit paid in or of a repayment of a debt.
>
> (...) If subsequently, in consequence of growing population and production, or the more extended use of money, more of the medium of exchange were required, this would be obtained quite simply by the bank increasing its discounting of bills or its lending in general, by which a corresponding amount of deposits would automatically flow in. The virtual velocity of circulation would thus tend to increase to infinity. A very small quantity of money would suffice for a very large business turnover.
>
> (...) The ideal banking system sketched above has in recent years engaged the attention of many writers under the name of "universal compatibilism," and various proposals for its realization have been made.

[43] "Knut Wicksell," Wikimedia Foundation. https://en.wikipedia.org/wiki/Knut_Wicksell.

[44] Knut Wicksell, *Lectures on Political Economy.* Vol. II: Money (G. Routledge and Sons, 1946), 87.

> (...) Theoretically this imaginary system is of extraordinary interest, in so far as it provides a very important means of appraising the factors influencing the value of money...[45]

Nowadays, this formulation does not seem so adventurous, given that not only do banks offer digital payment systems, and a large part of trade is conducted in this way, but also that currencies are no longer backed by precious metals or other commodities. Nevertheless, it is still considered a derivative of money in terms of backing and credit. This 'ideal bank' system is one in which reserves remain unchanged and either change ownership or do not exist, and all transactions are done by changing numbers in a spreadsheet or database. This idea will be illustrated in ethnographic cases from societies without written records and in social currency systems, which will also be useful for understanding the functioning of Bitcoin in the second part of this work.

◆ 1890 Austrian School: Logical Origin and Typology

In the last decades of the nineteenth century, Carl Menger (1840-1921), the last of the aforementioned founders of marginalist theory and founder of the Austrian school of economics, presented a more abstract theory on the origin of money, in a short article called, precisely, "On the Origin of Money."[46] Published in 1892, it was translated from an original in German simply titled *Geld* (Money) of the same year, of which I could not find a copy to properly quote. In this work, he did not attempt to make a historical or genealogical reconstruction, but merely to reach a logical conclusion as to why money appears in a society that exchanges goods. According to him, money arises spontaneously in an economy where different goods circulate because of the difference in their salability (*Absatzfähigkeit*). Economic agents, especially those who offer goods that are not very saleable, would tend to seek to exchange their goods not for those they ultimately need and are going to consume or use, but rather for those that are easier to sell later. Thus, little by little, these more sought-after goods will come to occupy a prominent place in the economy, as currency.

[45] Ibid., 84–87.

[46] Carl Menger, "On the Origin of Money," *The Economic Journal* 2, no. 6 (1892): 239–55.

Ludwig von Mises (1881-1973) is another major exponent of this school. He was educated by Eugen von Böhm-Bawerk (1851-1914), who, in turn, had studied with Bruno Hildebrand; however, he was mainly influenced by Menger. In 1912, he published *Theorie des Geldes und der Umlaufsmittel* [*Theory of Money and Credit*], a thorough analysis of various aspects of money. One of the most important contributions of this work was the clarification of the complicated relationship between the use value and exchange value of money.

The first two chapters address the definition of money and its key characteristics. Initially, he assigns it a single or principal function, "to facilitate the business of the market by acting as a common medium of exchange."[47] All other functions it may have, he says, "can be deduced from the function of money as a common medium of exchange."[48] The Austrian school, primarily represented by Menger and von Böhm-Bawerk, developed a subjectivist theory of value that should be synthesized to understand Mises's ideas. The idea of classical economics, which posits a labor-value and an objective use-value, is discarded; in its place, a subjective use-value emerges: each individual has his own scale of values at each moment or situation. Economic action (exchange or production) will be carried out whenever they decide that a particular good or service they can obtain is worth more than one they already possess. On this basis, Mises observes, "If it is impossible to measure subjective use-value, it follows directly that it is impracticable to ascribe 'quantity' to it."[49] The function of money as a measure of value is then ruled out. "Neither is objective exchange-value measurable, for it too is the result of the comparisons derived from the valuations of individuals."[50]

The third chapter of the first part, titled "The Various Kinds of Money," establishes a typology. It starts by making a fundamental difference:

> There are two sorts of thing that may be used as money: on the one hand, physical commodities as such, like the metal gold or the metal silver; and, on the other hand, objects that do not differ technologically from other objects that are not money, the factor that decides whether they are money being not a physical but a legal characteristic.[51]

[47] Ludwig von Mises, *The Theory of Money and Credit* (Mises Institute, 2009), 29.
[48] Ibid., 35.
[49] Ibid., 45.
[50] Ibid., 48.
[51] Ibid., 60

Here he differentiates between money in the strict sense and money substitutes. He then proceeds to detail three forms of money that are in the first category:

> We may give the name of *commodity money* to that sort of money that is at the same time a commercial commodity; and that of *fiat money* to money that comprises things with a special legal qualification. A third category may be called *credit money*, this being that sort of money which constitutes a claim against any physical or legal person.[52]

It is essential to consider that when this work was written, computers did not exist, nor was there a free-floating regime of national currencies. The money in circulation in each country had a value backed by that country's precious metal reserves. However, Chapter 2 of the third part of the book is titled "The Evolution of Fiduciary Media" and defines such a thing as follows:

> …fiduciary media are claims to the payment of a given sum on demand, which are not covered by a fund of money, and whose legal and technical characteristics make them suitable for tender and acceptance instead of money in fulfilment of obligations that are in terms of money (…).
>
> Fiduciary media may be issued in either of two ways: by banks, and otherwise. Bank fiduciary media are characterized by being dealt with as constituting a debt of the issuing body.[53]

The following table contains German, English, and Spanish terminology to avoid confusion when translating the concepts. It was elaborated using the English and Spanish versions of the work.[54] (The English version already contains a similar table, comparing the English and German terminology.)

[52] Ibid., 61.
[53] Ibid., 278.
[54] The English version is the one quoted throughout this work and the Spanish version is the 1936 edition from M. Aguilar. The English version contains the glossary at page 483.

Table .2: Mises's taxonomy for money in three languages.[55]

Geld im weiteren Sinne	Money in the broader sense	Dinero en sentido amplio
Geld im engeren Sinne	Money in the narrower sense	Dinero en sentido estricto
Geldsurrogat	Money substitute	Substitutivos del dinero
Sachgeld	Commodity money	Dinero-mercancía
Kreditgeld	Credit money	Dinero-crédito
Zeichengeld	Fiat money	Dinero-signo
Scheidemünzen	Token money	Moneda divisionaria
Geldzertifikat	Money certificate	Certificado de dinero

The critical thing to note is the difference between *fiat money*, *Fiatgeld*, or *Zeichengeld*;[56] and *fiduciary media* or *Umlaufsmittel*.[57] The former is a form of money in the strict sense imposed by law or a community, while the latter is a substitute for money in the form of a debt or promise of future payment. These concepts can be difficult to separate since the money in use today is both: national currencies are imposed by law in each country and backed by U.S. dollars, which are fiat money just like these, and at the same time, a fiduciary medium, since it is based on debt.[58]

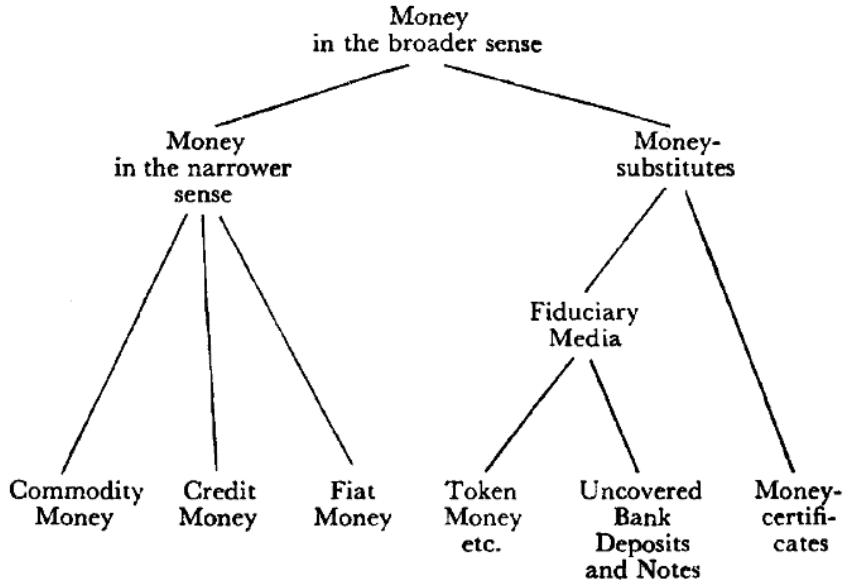
While Knapp considers that all money has its origin in law, he does not directly contradict Mises's theory. Yet, he reserves the name 'money' for a particular type of a larger category he calls 'medium of exchange'. For Mises, that function is what makes money, and he instead considers chartal money a particular form of money, namely, fiat money.

[55]Mises, *The Theory of Money and Credit*.

[56]From the Latin root *fiat*, past tense of the verb *facio*, which can be used as "to estimate" or "to value".

[57]From the Latin word *fiduciarius*, whose root is fide: faith, trust, loyalty.

[58]Robert P. Murphy, *Is our Money Based on Debt?* (Mises Institute, 2010).



In the second part, he addresses the fundamental question of the value of money, which was left unresolved by historical materialism prior.

> …while the utility of other goods depends on certain external facts (the objective use-value of the commodity) and certain internal facts (the hierarchy of human needs), i.e., on conditions that do not belong to the category of the economic at all but are partly of a technological and partly of a psychological nature, the subjective value of money is conditioned by its objective exchange-value, i.e., by a characteristic that falls within the scope of economics.
>
> In the case of money, subjective use-value and subjective exchange value coincide. Both are derived from objective exchange-value, for money has no utility other than that arising from the possibility of obtaining other economic goods in exchange for it.[59]

In this sense, the use-value of money is derived from the use-value of the goods for which it can be exchanged, using exchange-value. He distinguishes the objective exchange value of money from the price of money; the former is the possibility of obtaining certain goods in exchange for money, and the latter is the quantity of goods obtained with a unit of money.[60]

[59]Mises, *Theory of Money and Credit*, 97.
[60]Ibid., 101.

This proposition presents the challenge of explaining how the price of money is determined without falling into circular reasoning. The objective exchange value between any two commodities is determined by their relative use values and the law of supply and demand. Money, being also a commodity, should conform to this criterion, but its use-value depends, in turn, specifically on its exchange-value. Mises's explanation in this respect is that the first value of money is linked to the value of the commodity that officiates. From then on, both the first use value as a commodity and its use value as currency will influence its price by conditioning its supply and demand.[61]

> Before an economic good begins to function as money it must already possess exchange-value based on some other cause than its monetary function. But money that already functions as such may remain valuable even when the original source of its exchange-value has ceased to exist. Its value then is based entirely on its function as common medium of exchange.[62]

He considers this a reasonable basis for developing a complete theory of the value of money based on the subjective theory of value and marginal utility.

Although some postulates of the Austrian school became part of the hegemonic economic theories, such as Menger's contributions to the marginalist model, for the most part, it remained a heterodox school within economics. During the decades from 1930 to 1960, the leading capitalist countries adhered to Keynesian postulates. It was not until the 1970s that the Chicago school, with Milton Friedman as one of its primary proponents, adopted some Austrian tenets. The communist countries, for their part, followed the line of historical materialism or Marxist economics.

Twentieth-century economists have largely abandoned the debate on money and accepted some of the postulates explained above. To wit: Hildebrand's hypothesis was established as an almost mythical origin of money not subject to revision; Jevons's characteristics are mentioned in any basic introduction to the subject without mentioning its original author; and finally, Mises's typology is accepted as valid and complete. It would be necessary to wait until the twenty-first century for new theories of money to emerge, mainly due to the inability of the previous ones to

[61] Ibid., 109–10.
[62] Ibid., 111.

cope with some empirical contrasts. Several of these empirical cases will be presented in the following two sections, and later, in the last section of this first part, these new theories about money will be given.

Observation: Ethnographical, Ethnological, Anthropological, and Ethological Approaches

This is the first empirical section. It presents documented cases of monetary and credit systems in societies lacking formal governmental institutions, writing, or extreme living conditions, as well as beyond the human species, in studies carried out with other hominid primates.

It also contains some theoretical developments or criticisms of the economic schools, which were made based on these empirical data. Although a complete theory of money and currency has not been formulated, the debate that the proper economic schools abandoned has been renewed. In the second theoretical part, I will explain the reflection that these criticisms provoked within economic science.

The most important work for this section is that of Paul Einzig, whose collection of ethnographies is perhaps the most complete available about currency and money. The intention in selecting examples was to cover the broadest range of manifestations of monetary and money phenomena in order to test the abstract and general postulates reviewed in the previous section.

◆ On the Antiquity of Currency. Trading with Monkeys

While simple evolutionism, such as Hildebrand's, was abandoned by social scientists long ago, questions about the origins and antiquity of many technological advances and various human institutions are a field of study that is still valid today and has made significant discoveries since Thomsen.

Historians (if we hold to the traditional concept that the discipline is concerned with collating written sources and that history begins with writing) have come across that the earliest written sources, in Mesopotamia, were related to the logistics and economics of the civilizations that produced them. Inventories and logistics are not the same as money, and the evidence for the existence of money in that period (3500-2250 B.C.) and in those societies is almost nil.[1] Only the Hammurabi Code (1754 B.C.) explicitly references money, wages, fines, payments, debts, and other related matters. From this perspective, although a very ancient invention, money has only emerged after other technological advances, such as agriculture, writing, the State, and laws. In short, money might seem to have appeared after written history had started. Ethnography, however, as I will demonstrate throughout this chapter, has provided substantial evidence that a writing system and a centralized, efficient state organization are not prerequisites for the existence of a monetary system within each community. In this sense, currency and money are part of the inventory of human prehistory. It may take a detailed study of ancient civilizations, such as those of Mesopotamia, Egypt, and the Incas of South America, to demonstrate that their outstanding achievement regarding money was not to have used it to control their enormous economies. However, that is beyond the purpose of this work.

Before dealing with human prehistory proper, we can go back further than our own species. Communication and the possibility of speech in our evolutionary history have been studied through experiments and observations of communication in groups of primates closely related to us, *Homo sapiens sapiens*. Similarly, there is an extensive bibliography of experiments on the use of currency by other primates. According to this evidence in this first chapter, I want to present just how ancient in the

[1] Ancient History Encyclopedia s.v. "Writing Timeline."

evolution of hominids is the possibility, at least in the cognitive field, of understanding the concept of money.

The earliest work in this regard was published by Kohts in 1935,[2] a year before Wolfe,[3] who was simultaneously studying the same topic elsewhere, namely the cognitive abilities of chimpanzees. More recent experiments used capuchin monkeys (*Cebus apella*) instead of chimpanzees. The first one I will quote proposes that "the use of tokens by a capuchin to make communicative requests for specific context-dependent tools would provide evidence for representational intelligence in the instrumental behavior of this species."[4] To test this, they carry out five more complex experiments in which the test subject, Virgil, is presented with colored tokens; in exchange, he receives tools to procure food in specific tasks. The results are that "Virgil's chip selection strategy was consistent with an ability to recognize a task, determine which tool was appropriate for that task, recall the chip associated with the appropriate tool, and then use the chip to make a communicative request."[5] There is first evidence that these monkeys can symbolize and understand that a token of a particular color is worth a specific tool.

In a second series of experiments, the same team of researchers tested the ability of these primates to recognize and act appropriately in bartering situations:

> We presented subjects with opportunities to obtain various foods and a tool from an experimenter in exchange for the foods or tool in the subjects' possession. (…) The subjects demonstrated the ability to recognize that exchanges could occur when an experimenter was present with a desirable food. (…) These results indicate that tufted capuchins recognize opportunities to exchange and engage in a simple barter system whereby low-valued foods are readily traded for more highly valued food. Furthermore, these capuchins demonstrate that their value for a tool changes depending upon its utility.[6]

[2]Nadezhda Nikolaevna Ladygina-Kohts, *Infant Chimpanzee and Human Child: A Classic 1935 Comparative Study of Ape Emotions and Intelligence*, (Oxford University Press, 2002).

[3]John Bascom Wolfe, *Effectiveness of Token Rewards for Chimpanzees* 12, no. 60, (Comparative Psychology Monographs 1936).

[4]Gregory C. Westergaard et al.,"Token-mediated Tool-use by a Tufted Capuchin Monkey (Cebus apella)," *Animal Cognition* 1 (1998): 101–06.

[5]Ibid., 105.

[6]Westergaard et al. "Tufted Capuchins (*Cebus apella*) Attribute Value to Foods and Tools During Voluntary Exchanges with Humans," *Animal Cognition*, 7 no.1 (2004): 19.

> This characteristic of capuchin behavior has not been previously demonstrated in New World primates and suggests that this capacity is not unique to the ape/human lineage.[7]

In a third instance, they wanted to see if they could exchange tools with each other instead of with a human experimenter by means of tokens.

> Using a similar set of tokens and objects to those employed in the previous study, we tested whether our original subject and a conspecific with similar training could use tokens to obtain situation-appropriate tools from each other. Our primary interest was to test whether the monkeys could generalize their token training with the experimenter to tasks requiring token exchanges with a conspecific. Also, of interest was whether or not the monkeys could reverse roles in the token exchange paradigm without explicit training in an opposite role.[8]

The results were not entirely encouraging:

> Our findings suggest that, although capuchins are able to learn specific token-object relationships, they may be unable to use tokens to obtain specific objects from conspecifics.
>
> (...) the capuchins did not transfer situation-appropriate tools to a conspecific following the transfer of a specific token. This result contrasts with the ability of great apes to satisfy conspecifics' symbolic object requests (Savage-Rumbaugh et al. 1978a, b). Each capuchin's performance in exchanges with a conspecific suggests that their token abilities were fully generalized only to the token transfer role, and not to the less familiar, tool transfer role. (...) Presumably, because of this limitation, the capuchin monkeys' capacity for token exchange was unidirectional. (...) Successful training of capuchin monkeys in both roles of this paradigm will allow for more sophisticated research with this species within the realm of token exchange.[9]

The chimpanzee work he cites consisted of the following:

> Two chimpanzees have demonstrated the ability to learn to use graphic symbols to ask one another for tools needed to obtain food.

[7] Ibid., 24.

[8] G.C. Westergaard, Theodore Avery Evans, and Sue Howell, "Token Mediated Tool Exchange Between Tufted Capuchin Monkeys (*Cebus apella*)," Animal Cognition 10 no.4 (2007): 407–14.

[9] Ibid., 413–14.

> The chimps readily attended to and complied with one another's requests by selecting the appropriate tool from six distinct alternatives. They then shared the food obtained by this means and readily reversed the roles of tool requester and tool provider. (...) The acquisition of tool names revealed that words are at first closely and concretely linked to function, and hence that the traditional object-naming paradigm alone is a comparatively difficult starting point for the chimpanzee.
>
> This work has demonstrated that two chimpanzees have been able to comprehend the symbolic and communicative function of the symbols they use.[10]

All the studies cited so far, while indicative of a symbolic capacity of other primates to understand that a token is worth an object and to value them, have assigned different tokens to each object rather than different quantities of the same token.

A subsequent experiment dealt with this and took a large group of capuchins as test subjects.

> Twenty-eight captive-born capuchin monkeys (...) participated in the study. We divided our subjects into 2 rank classes (Drea and Wallen 1999; Schino 2004) on the basis of aggressive interactions, submissive behaviors, and access to food at feeding time (Verbeek and de Waal 1997).
>
> (...) We tested 18 knowledgeable subjects and 10 naïve subjects. Of the 18 knowledgeable subjects, 11 (4 high-ranking and 7 low-ranking) had previously learned to exchange the 2 types of tokens used in the present study, i.e., high- and low-value tokens (...). The 10 naïve subjects had never been observed to exchange any object spontaneously nor had they witnessed their group members exchanging tokens before this study.
>
> We assigned to each knowledgeable subject 3 different objects as low-value, high-value, and no-value tokens. The low-value tokens corresponded to 1 reward, while the high-value tokens corresponded to 3 rewards; a reward consisted of 1/8 of a peanut.[11]

[10] E. Sue Savage-Rimbaugh, D.M. Rumbaugh and S. Boysen, "Linguistically Mediated Tool Use and Exchange by Chimpanzees (*Pan troglodytes*)," Behavioral Brain Science 1 Mo. 4 (1978): 539.

[11] Elsa Addessi, Alessandra Mancini, Lara Crescimbene et al., "How Social Context, Token Value, and Time Course Affect Token Exchange in Capuchin Monkeys (*Cebus apella*)," *International Journal Primatology.* 32 No. 1 (2011): 83–98.

In this case, the difference between the types of cards is quantitative rather than qualitative, and they are comparable and fungible. The results were as follows:

> Social status affected exchange behavior. All 6 naïve subjects that exhibited token exchange during this study were high-ranking individuals, whereas all 4 that did not were low-ranking individuals (Fisher's exact, $p<0.01$). High-ranking individuals exchanged significantly more tokens and other items than low-ranking ones (Mann Whitney U test: $Z=3.74$, $n1=10$, $n2=18$, $p<0.001$; $Z=2.07$, $n1=10$, $n2=18$, $p=0.04$; Fig. 1). However, token availability did not seem to affect the behavior of low-ranking individuals.[12]
>
> Social context had both positive and negative effects on individual behavior (Fragaszy and Visalberghi 1990). Six of 10 naïve subjects exchanged tokens in the initial sessions, and across sessions they behaved similarly to knowledgeable subjects.
>
> (...) In the present study, the effect of the social context on the acquisition of token exchange by naïve individuals depended on their hierarchical rank: Whereas the presence of group members was effective in prompting the acquisition of token exchange behavior by high-ranking naïve subjects, it impaired learning by low ranking naïve subjects. (...) Although all 18 knowledgeable capuchins proved to be highly motivated and skillful token exchangers when individually tested (Addessi et al. 2007, 2008a, b), 10 of them, all low-ranking individuals, never displayed token exchange in the social context. In addition, high-ranking individuals, regardless of whether they were knowledgeable or naïve, monopolized the experimenters and exchanged more tokens, regardless of their value, and other items than low-ranking individuals. They often brought multiple tokens from the indoor compartment to the outdoor compartment, accumulated them in front of the experimenter, and then exchanged them 1 at a time. (...)
>
> Capuchins exploited their token budget as soon as the opportunity arose. (...) In contrast to our expectations, capuchins did not exchange tokens more than other items, possibly because wooden chips, twigs, and stones were dramatically more abundant and ubiquitous than tokens, being enrichment devices entirely covering the ground of the outdoor compartments. Moreover, "trading *per se*" might be sufficient motivation for the animals to continue exchanging (Car-

[12] Ibid., 91.

> penter and Locke 1937, p. 273). In fact, although exchanging no-value tokens or other items does not lead to a food reward, this is probably an intrinsically motivating behavior, i.e., an activity that is performed for its own sake (Deci and Ryan 1985), especially for high-ranking individuals that monopolized access to the experimenters (...) when social factors do not limit token availability and access to tokens, capuchins are able to exploit tokens according to their value.
>
> (...) Interestingly, capuchins learned over time to leave tokens in the indoor compartment, where the experimenters originally placed them, until it was time for exchanging, instead of carrying and spreading tokens outdoors, where the probability to lose them is high. (...)These findings might suggest the development of very basic token saving strategies, though certainly less sophisticated than reported by Sousa and Matsuzawa (2001) for chimpanzees. In the latter study, in which tokens were used as rewards in cognitive tasks, all chimpanzees spontaneously saved tokens, thus showing that, at least in a brief time interval, they can plan a future action and delay gratification. However, contrasting evidence is provided by the study of Dufour and Sterck (2008), in which no chimpanzees systematically selected the specific object required to later perform a series of exchanges with the experimenter. (...) Finally, capuchins recognized that the experimenter's presence was a *condicio sine qua non* for token exchange to be successful, although they could not restrain from exchanging whatever object was available, regardless of its value.[13]

These results are interesting in several aspects, including social stratification and inequality, as well as exchange as a recreational activity, etc. Still, as far as this work is concerned, they demonstrate one thing: that the aptitude for trade and the development of currency as a tool is of great antiquity in our evolutionary history. The separation between the *Platyrrhini* taxa (to which capuchins belong) and *Catarrhini* (to which we hominids belong) is estimated at thirty-five million years and that of *homo* (to which we humans belong) and *pan* (to which chimpanzees belong) between 5 and 7 million years.[14] In other words, the cognitive abilities to handle a means of exchange were probably present before humans developed bipedalism

[13] Ibid., 93–95.

[14] Carlos G. Schargo, "Timing the Origin of New World Monkeys," *Molecular Biology and Evolution* 20, no. 10 (2003): 1620–25.

and currency could have been invented at any time during the evolution of the genus *homo*.

◆ 1875 Jevons: An Early Ethnology

As I commented in a previous chapter, Jevons considered the various forms money has taken in the record of history and diverse cultures and devoted an entire chapter to the exposition of them.

> …every kind of merchandise has the two properties of measuring value and transferring value. It is entirely a question of degree what commodities will in any given state of society form the most convenient currency, and this truth will be best impressed upon us by a brief consideration of the very numerous things which have at one time or other been employed as money.[15]

Following the conventions of his time's unilineal and stadial evolutionism, he considered currency to be associated with a society's degree of development, like Hildebrand, Morgan, Marx, and Hegel. Thus, he identifies one type of currency for hunter-gatherer societies, another for pastoral societies, and a third for the agricultural state or ancient civilization.

He begins by establishing that in a hunting society, the fruit of such activity provides the most valuable materials, and since meat is perishable, skins are the rudimentary form of currency. His sources include biblical passages, the etymology of certain Slavic words related to money and fur, historical records, travel diaries, and records of colonial companies that traded with North American tribes.[16]

For the second stage, pastoral society, it is no longer furs but whole animals that constitute the form of money. His main sources are the Homeric poems, in which the value of objects is often referred to in terms of oxen; although precious metals also appear, they are reserved as forms of storing value rather than currency. He also cites linguistic convergences between the terms for currency and livestock in Latin and Anglo-Saxon languages to support his argument. In addition, he adds that in slave societies, some of which are contemporaries of his own, particularly in Central Africa, enslaved people are a medium of exchange along with cattle and ivory.

[15] Jevons, *Money and the Mechanism of Exchange*, 19.
[16] Ibid., 20-21.

Additionally, in this regard, he cites a New Guinean source that states slaves were a medium of exchange in trading circles, and there is a vague notion that, at some point in history, slaves were also used as common currency in England.[17]

In the third place, in agricultural societies, various products of this activity serve as a form of currency. Jevons states that wheat, oats, barley, nuts, cocoa, and corn were used in Europe and Mesoamerica during ancient times to make payments and loans. Similarly, olive oil was used around the Mediterranean and in the Levant. His sources are certain documents on colonial trade. He even recovers some laws from the British colonies as late as the 17th and 18th centuries, in which products such as tobacco and corn were declared legal tender. In the western islands of India, on the other hand, he finds a document of a trial in which a person is forced to accept various products such as sugar, rum, molasses, ginger, indigo, or tobacco as payment. Finally, he discusses eggs used as currency in Switzerland and stuffed fish in Newfoundland and North America, yet he does not cite any sources.[18]

Lastly, he also reviews ornamental objects and manufactured items used as coins. He mainly names *wampumpeag*, "beads made of the ends of black and white shells, rubbed down and polished, and then strung into belts or necklaces which were valued according to their length, and also according to their colour and lustre."[19] According to seventeenth-century sources, the colonists traded with the natives, and official exchange rates were established between the two currencies.

> Exactly analogous to this North American currency is that of the cowry shells, which, under one name or another—chamgos, zimbis, bouges, porcelanes, etc.—have long been used in the East Indies as small money. In British India, Siam, the West Coast of Africa, and else where on the tropical coasts, they are still used as small change, being collected on the shores of the Maldive and Laccadive Islands, and exported for the purpose. (…) Among our interesting fellow-subjects, the Fijians, whale's teeth served in the place of cowries (...).

[17] Ibid., 21–24.
[18] Ibid., 25–27.
[19] Ibid., 24.

> Among other articles of ornament or of special value used as currency, may be mentioned yellow amber, engraved stones, such as the Egyptian scarabsei, and tusks of ivory.[20]

Among manufactured items, he mentions Guinea pieces in addition to other fabrics, straw, salt, benzoin gum, beeswax, red feathers, tea, shovels, hoes, and nails, all of which were generally recorded during the colonial period and throughout the world. Finally, he mentions an alleged wooden money used by the Byzantines, about which he has little information. He advances a hypothesis about prehistoric lithic objects found far from their place of origin, which may have circulated as money.[21]

◆ 1914-1924 Marcel Mauss: First Comprehensive and General Approach to Currency

Ethnology at the beginning of the twentieth century also began to approach the problem of money from a genealogical approach, seeking to reconstruct a history and searching for an origin. In this line we find, for example, the work of Schurtz: *Grundriss einer einer etstehungsgeschichte des geldes (Foundations for a History of the Origin of Money)*,[22] not translated. But it is Marcel Mauss who, in 1914, gave the guidelines for a more structural approach: "in which form the most primitive, the simplest, the most elementary, to say better, one can imagine that was presented, in the lowest societies that we know, the concept of money."[23]

This work by Mauss, *Les origines de la notion de monnaie (The Origins of the Notion of Money)*, is relatively brief.[24] Still, it contains fundamental concepts and guidelines to understand his subsequent approaches in his most important work. Before turning to that major work, I will review the ideas presented in this, more modest, one.

Mauss first points out that "Currency is by no means a material and physical fact, it is essentially a social fact; its value is that of its purchasing

[20] Ibid., 24–25.
[21] Ibid., 27–29.
[22] Heinrich Schurtz, Grundriss Einer *Etstehungsgeschichte des Geldes* (E. Fleber, 1898).
[23] Marcel Mauss, "Les Origines de la Notion de Monnaie," *Comptes-Rendus Séances* 1 No. 2 (1914): 14–19.
[24] Unfortunately, there is no English version of this work, so I will quote the original French version.

power, and the measure of the confidence one has in it."[25] And that "it is not a question of showing an origin, which is to say an absolute beginning, a birth so to speak *ex nihilo*."[26] While economists such as Menger had already set aside the genealogical perspective in favor of a more functional one, they considered currency and exchange as an autonomous sphere, clearly defined and separate from the other spheres of social activity. It is at this point that the anthropological perspective makes the difference. Mauss advances the notion that there is a close relationship (which he highlights in the linguistic and semiotic terrain) between magical power, prestige, authority, and economic power. He gives numerous examples taken from ethnographies of Melanesia and North America to conclude that "we have hardly found any society, sufficiently close to the origins, where the cult and the magic of stones, shells, and precious metals have not given a real value to these objects."[27] Conversely, he not only tries to find the religious in the economic, but also the economic in the religious activity:

> ...we have the proof that not only religious facts, but also economic facts must be seen in the pilgrimages with exchange and trade, (...) these visits entail many gifts: food, use of women, etc., or they are made on their occasion.[28]

Ultimately, he defines the currency as follows:

> The currency, - whatever the definition one adopts - is a standard value, it is also a use value which is not fungible, which is permanent, transmissible, which can be the object of transactions and uses without being deteriorated, but which can be the means of obtaining other fungible, transitory values, enjoyments, benefits. Now the talisman and its possession have, as far as we are concerned, very early on, undoubtedly from the most primitive societies, played this role of objects equally coveted by all, and whose possession conferred on their holder a power which easily became a purchasing power. (…) The purchasing power of primitive money is above all, according to us, the prestige that the talisman confers on the person who possesses it and who uses it to command others.[29]

[25] Mauss, "Les Origines de la Notion de Monnaie," 3.
[26] Ibid., 4.
[27] Ibid., 6.
[28] Ibid., 7.
[29] Ibid., 7–8.

Ten years later, he published one of his most important works: *Essai Sur le Don (Essay on the Gift).* Chapter 2, which is titled "The Extension of this System: Liberality, Honour, Money," will be used in this study. The book is about exchange, but he approaches this topic in a non-economistic way. Perhaps because he was against the idea of a social life governed by mercantile logic, his perspective on the matter can be illustrated by the following quotation:

> In short, this represents an intermingling. Souls are mixed with things; things with souls. Lives are mingled together, and this is how, among persons and things so intermingled, each emerge from their own sphere and mixes together. This is precisely what contract and exchange are.[30]

This concerns exchange in general, which, as I mentioned earlier, Mauss attempts to situate as an integral part of social life, rather than as an isolated activity, and certainly not as the primary element of social life. Concerning this work, David Graeber states that:

> [It] was written in response to the crisis of socialism he saw in Lenin's reintroduction of the market in the Soviet Union in the '20s: If it was impossible to simply legislate the money economy away, even in Russia, the least monetarized society in Europe, then perhaps revolutionaries needed to start looking at the ethnographic record to see what sort of creature the market really was, and what viable alternatives to capitalism might look like.[31]

While economists like Menger and Mises studied money to perfect capitalism, Mauss, like Marx, did so to find an alternative to it.

He debates with Malinowski over the case of the Trobriand Islanders, as Mauss has a broader conception of what a currency is. He develops this dispute in an extensive footnote, which is quite common among his works:

> Malinowski has previously protested against the abuse of the term [currency] (Argonauts, p. 499, n. 2), and has criticized Seligmann's nomenclature. He reserves the notion of money for objects that not only serve as a means of exchange, but also as a standard to measure value. (...)

[30] Marcel Mauss, *The Gift. The Form and Reason for Exchange in Archaic Societies* (Routledge Classics, 2002), 25–26.

[31] David Graeber, *Fragments of an Anarchist Anthropology* (Prickly Paradigm Press, 2004), 17.

On this reasoning there has only been economic value where there has been money, and there has only been money when precious things, themselves intrinsic forms of wealth and signs of riches, have been really made into currency, namely, have been inscribed and impersonalized, and detached from any relationship with any legal entity, whether collective or individual, other than the state that mints them. (...) In my view, one only defines in this way a second type of money—our own.

In every society that has preceded those in which gold, bronze, and silver have been minted as money, there have been other things, stones, shells, and precious metals in particular, that have been used and have served as a means of exchange and payment. In a fair number of societies around us today this self-same system functions in reality, and it is this one we are describing.

Figure 2. *Mwali* from Trobriand. Source: Pinterest.

It is true that these precious objects differ from what we are accustomed to conceive of as instruments for discharging debts. First, in addition to their economic nature and value, they have also a somewhat magic nature and are above all talismans (...). Their value is still subjective and personal. (...) It is still true that these values are unstable, and lack that character of being a standard or measure. For example, their price rises or falls with the number and size of the transactions in which they have been used. Malinowski very neatly compares with the jewels in a crown the *vaygu'a* of the Trobriand, which acquire prestige in the course of their voyages. Likewise, the emblazoned copper objects of the American Northwest and the mats of Samoa increase in value at each potlatch and in each exchange. On the other hand, from two standpoints, these precious objects have the same function as money in our societies and consequently deserve at least to be placed in the same category. They have purchasing power, and this power has a figure set on it.

(...) The idea of number is present, even if that number is fixed in a different way from the authority of the state, and varies during the succession of kula and potlatches. Moreover, this purchasing power does indeed discharge debts. Even if it is recognized only between individuals, clans, and certain tribes, or only between associates, it is nonetheless public, official, and fixed.[32]

[32]Mauss, The Gift, 29.

Although I agree with the first part (one cannot call currency only the symbol minted by a state authority), as would any of the theorists whose ideas I explored in the previous section, except Knapp; it seems to me that the breadth he gives to the concept is excessive for one reason: the fundamental thing about a currency is not to have a quantifiable purchasing power, but to be the object of general exchange. While Mauss does account for the fact that *kula* exchange is ceremonial and solemn, and that in parallel, *gimwali*, which is a mundane form of exchange, takes place, he does not find it relevant that the *vaygu'a* of the *kula* are apart from the *gimwali*. This indicates that the *vaygu'a* are not currencies, not even a currency limited to the nobility, since they are only exchanged for other *vaygu'a*.

Further on, he even states that "Through gifts made and reciprocated, they have robustly replaced a system of buying and selling."[33] This renders a currency practically useless. Yet the reasoning by which Mauss arrives at determining what makes a currency is not that of seeking the place that a monetary element can have in each system of exchange. Instead, he seeks to define how different concepts of the economy and law of his complex society are emerging from a sort of primordial chaos whose remnants he finds in primitive societies. He even develops his own version of the three stages of the evolution of currency.[34] Ultimately, what happens with Mauss is that currency is not the main object of his analysis. Rather it is only one element among others, and, therefore, it is only relevant to him insofar as it explains *systems of 'total services'* He describes how the entire economy is articulated based on moral obligations and how precious objects (goods that have little or no use value but concentrate exchange value) are intrinsic to these systems. However, he does not explain clearly or in detail how these precious objects, these currencies, are used for exchange in these systems. Ultimately, he focuses his analysis elsewhere.

Figure 3. *Soulava* from Trobriand. Source: Pinterest.

[33]Ibid., 41.
[34]Ibid., 100.

Figure 4 : *Kwakwaka'wakw* (Kwakiutl) copper. Source: Sasamans Society.

The next section of his book is subtitled "Honour and Credit,"[35] which focuses on the tribes of North America, since "two notions are much more in evidence than in the Melanesian *potlatch* or the more developed, or more fragmented, institutions existing in Polynesia. These are the notion of credit, of the time limit placed on it, and also the notion of honour."[36] He quotes the following from Franz Boas in a note from this page.[37] "The Indian has no system of writing and consequently, to guarantee the transaction, the promise is made in public."[38] This fact will be fundamental later in understanding how blockchains work and how they return to this point in a certain way. But returning to Mauss, what he will point out above all is the error of Hildebrand's conception of the evolution of exchange systems, not so much to deny the notion of unilinear evolutionism but, one might say, to reorder its stages, as pointed out before:

> …the gift necessarily entails the notion of credit. The evolution in economic law has not been from barter to sale, and from cash sale to credit sale. On the one hand, barter has arisen through a system of presents given and reciprocated according to a time limit. This was through a process of simplification, by reductions in periods of time formerly arbitrary. On the other hand, buying and selling arose in the same way, with the latter according to a fixed time limit, or by cash, as well as by lending.[39]

Honor is often associated with wealth because it is often obtained through spending and making large donations. It is not by hoarding wealth that one climbs the social ladder, but by squandering it, paying off debts, and ultimately putting others in debt, that is, by hoarding credit. This is the obligation to give.[40]

[35] Ibid., 42.
[36] Ibid., 45.
[37] The English version has the notes of each chapter at the end, as in English quotation. The French and Spanish versions have them in their original form, as footnotes.
[38] Mauss, *The Gift*, 100.
[39] Ibid., 46–47.
[40] Ibid., 50.

On the other end, the receiving party cannot easily refuse a gift given to him, since as that gift is a challenge, he would be cowering and implying that he is not up to the task of entering into this back-and-forth of gifts. That would lead him to lose his honor from the beginning, except for certain exceptions in which it means the opposite: that the offeror is inferior and cannot give anything to the one stationed above him.[41]

Lastly, there is the obligation to reciprocate:

> …normally, the *potlatch* must be reciprocated with interest, as must indeed every gift. The rate of interest generally ranges from 30–100 per cent a year. (...) The punishment for failure to reciprocate is slavery for debt.[42]

Later in that chapter, Mauss returns to the problem of precious and sacred objects, although he does not call them 'currency' on this occasion:

> …in the things exchanged during the potlatch, a power is present that forces gifts to be passed around. (…) They are loans rather than sales or true abandonment of possession. (…) The sum total of these precious things constitutes the magical dower. (…) Each of these precious things, these signs of wealth possesses —as in the Trobriand Islands— its individuality, its name, its qualities, its power. (…) Each one of these precious things possesses, moreover, productive power itself. It is not a mere sign and pledge; it is also a sign and a pledge of wealth, the magical and religious symbol of rank and plenty. (…) things are mixed up with spirits, their originators, and eating instruments with food.[43]

Figure 5. *chilkat* fabric. Source: Wikipedia.

In short, these precious objects symbolize the identity of families, supernatural beings, rank, honor, or other things (that is what the author means when he says that they are 'confused with'). This may lead to the concept of 'fetishism,' which was discussed earlier, but will be elaborated on later. As mentioned earlier, the example of the capuchin monkeys reveals how ancient this symbolic capacity is in evolutionary terms.

[41] Ibid., 52.
[42] Ibid., 53–54.
[43] Ibid., 55–57.

Finally, Mauss returns to the currency, but the 'money of fame' (*Renommiergeld*), referring to the Haida and Kwakiutl emblazoned coppers.

> …when one considers both the copper objects and the other permanent forms of wealth that are likewise an object of hoarding and of alternating potlatches, masks, talismans, etc.—all are mingled together as regards use and effect. Through them one obtains rank; it is because one obtains wealth that one obtains a spirit. The latter, in its turn, takes possession of the hero who has overcome all obstacles. Then again, this hero has his Shaman trances, his ritual dances, and the services of his government [sic] paid for him. Everything holds together, everything is mixed up together. Things possess a personality, and the personalities are in some way the permanent things of the clan.
>
> (...) The circulation of goods follows that of men, women, and children, of feasts, rituals, ceremonies, and dances, and even that of jokes and insults. All in all, it is one and the same. If one gives things and returns them, it is because one is giving and returning 'respects'—we still say 'courtesies'. Yet it is also because by giving one is giving oneself, and if one gives oneself, it is because one 'owes' oneself—one's person and one's goods—to others.[44]

Again, calling these objects currency has little to do with their being a good that can be exchanged for all other goods in circulation. He calls them currency because they symbolize circulation, among other things, in the same way that coins, in the mercantile sense, represent the potential possession of any goods in circulation. And, again, currency itself is not the object of Mauss's study, as can be seen in the conclusions of this chapter:

> *…this principle of the exchange-gift must have been that of societies that have gone beyond the phase of 'total services'* (from clan to clan, and from family to family) *but have not yet reached that of purely individual contract*, of the market where money circulates, of sale proper, and above all *of the notion of price reckoned in coinage weighed and stamped with its value.*[45]

He conceives that there is currency even if there is no money, which may seem contradictory if we consider that they are the same thing. Later, I will present the ideas of another author that clarify this point.

[44] Ibid., 58–59.
[45] Ibid., 59.

◆ 1924 Armstrong: Shell Credit System

In the same year that Mauss's book was published, Armstrong published an early and detailed ethnography of a monetary system on Rossel Island in Papua New Guinea.[46] According to the author, this economic system has particular and striking characteristics different from those of the rest of the region. There are coins made with perforated shellfish discs joined with thread. Furthermore, a coin is not an individual disk but a set of several. These coins are divided into two large groups (*Dap* and *Kö*), each with different denominations for the values. Armstrong numbers them from lowest to highest (number 1, number 2, etc.); nevertheless, he clarifies that:

> In nearly all instances of real money throughout the world, where there are coins of different values, a higher value coin is generally regarded as equivalent to so many of the lowest value coins or at least as being composed of so many recognised units of value. This is not the case on Rossel; the value of a coin x in terms of a coin y is expressed by the length of time y would have to be let out on loan in order that x be repayable.[47]
>
> ...it distorts the facts to say that there is a definite rate of interest. It is better, therefore, to substitute for the statement that x is k times a No. 1 the statement that x is a No. 1 of so many months ago, which brings in a second unit of value, time. The common denomination being understood, then the price of any commodity or service might be put in terms of time, e.g. "a wife costs a year, a house two years, a basket of taro a week, and so on."[48]

[46] Despite the proximity of the two publications, Mauss cites Armstrong's work. See, for example, note 29 of chapter 2 cited above.

[47] W.E. Armstrong, "Rossel Island Money: A Unique Monetary System," The Economic Journal. 34, No. 135 (1924): 423–29.

[48] Ibid., 427.

Figure 6: Da por Ndap coin No. 3 '*Kejem*' offered on an Internet trading site. Source: Worthpoint.

Another peculiarity is that a constant number of coins is passed from person to person in transactions, and no new coins are produced beyond the first six or seven lowest denominations, nor are they taken out of circulation. Thus, coins have a value related to their antiquity, to an ancestral and mythical antiquity. In fact, the coins that make up the higher value classes each have their own name in addition to that of the classes to which they belong. The most valuable categories do not even circulate but are treasured and inherited by the most important families of the island.

> At the present day, No. 18, of which there are twenty coins on the island, is involved in payments for wives, for "ptyilibi" (polyandric wives) and pigs. When a No. 18 passes from person to person, it is handled with great reverence, and a crouching attitude is maintained. Nos. 19 to 22 are so sacred that they are always kept enclosed and are not supposed to see the light of day. Apparently they have little or no work to do now, except as security, and are owned only by chiefs. No. 22, of which there are seven coins, is inherited in the male line; and, apparently, the chiefs who own these are the most important on the island.[49]

He also explains that the handling of these currencies has made its place in the division of labor in that society:

> The borrowing and lending of coins is, in fact, so important that there exists a special class of persons who act as agents for these transactions; they are denoted by a special name, which may be translated by the term "broker" without much change of sense.[50]

There also appears the question of the security of transactions through attestation, pointed out by Mauss:

> …even when a single low-value coin is borrowed, it must be touched by a number of people, who, as witnesses, act as a safeguard to the lender.[51]

[49] Ibid., 428.
[50] Ibid., 427.
[51] Ibid., 428.

This brief ethnography ends as follows:

> In conclusion, it may be pointed out that Rossel Island money is money in the strict sense of the term. It serves as a medium of exchange and a standard of value, and it is not desired for its utility for other purposes, even for ornament or display. Indeed it is even considered "bad form" to make any sort of display of one's wealth of Dap and Kö.[52]

◆ 1949-1966 Einzig: Exhaustive Compendium of Ethnographies on Money

Paul Einzig was a writer and journalist of Hungarian Jewish origin, based in England, who held a doctorate in political science and economics from the University of Paris. He mainly wrote articles in newspapers such as the *Financial Times* (at that time called *Financial News*). Among his works is an extensive compilation volume of ethnographies on money, titled *Primitive Money: In Its Ethnological, Historical, and Economic Aspects*, first published in 1949 and followed by a revised edition in 1966. According to his introduction, his motivation was the following:

> For some time past I had felt that the early phases of the evolution of money had not been dealt with adequately either by economic history or by anthropology, and least of all by economic theory. (...) I felt a strong desire to probe into a question raised by Keynes in his *Treatise on Money*—whether in the distant past the inadequacy of the monetary system had ever hindered the progress of mankind in the same way as it had in recent times.[53]
>
> And I strongly felt the need for supplementing and correcting some existing theories, and even for replacing some of them. (…) Furthermore, I felt the need for putting forward a "social theory" of money, under which money is regarded not as a technical instrument but a social institution providing the driving force in primitive and modern communities alike, even though in a different way. Finally, I had to fill some blanks by elaborating some new theories peculiar to the working of primitive money.[54]

[52] Ibid., 429.
[53] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, xv.
[54] Ibid., xvi.

On the other hand, the second edition was motivated by the need to document the cases of primitive money before they disappeared due to the expansion of modern systems of printed money. In it, he added several sections and reflections, of which he considers the one dealing with this replacement to be the most important.

The work is structured as follows:

- BOOK 1: ETHNOLOGICAL SECTION
  - PART I. OCEANIA
  - PART II. ASIA
  - PART III. AFRICA
  - PART IV. AMERICA
- BOOK II: HISTORICAL SECTION
  - PART I. ANCIENT PERIOD
  - PART II. MEDIEVAL PERIOD
  - PART III. MODERN PERIOD
- BOOK III: THEORETICAL SECTION
  - PART I. WHAT IS PRIMITIVE MONEY?
  - PART II. THE ORIGIN OF MONEY
  - PART III. THE VALUE OF PRIMITIVE MONEY
  - PART IV. THE FUNCTIONS OF PRIMITIVE MONEY
  - PART V. PRIMITIVE MONETARY POLICY
  - PART VI. THE PHILOSOPHY OF PRIMITIVE MONEY

Each part contains several chapters. In the case of the first book, each chapter reviews a single ethnography; there are fifty-three, with thirteen per part. How he defines *primitive money* is as follows:

> ...a unit or an object conforming to a reasonable degree to some standard of uniformity, which is employed for reckoning or for making a large proportion of the payments customary in the community concerned, and which is accepted in payment largely with the intention of employing it for making payments.[55]

[55] Ibid., 317.

And the distinction between money and currency:

> The two terms are often used indiscriminately, while the discrimination between them is unreasonable. To the author's mind, "currency", as its name implies, is "current money", that is, money actually in physical circulation, or capable of being put into circulation. Credit-money does not belong to this category, nor do abstract units of account. Both are money, but they are not currencies. Every currency is money, but only those moneys which are actual circulating media are currencies.[56]

Einzig includes the cases presented to him according to these definitions since many do not conform to orthodox economic definitions of money.

Two cases he includes will be outlined here for two reasons: first, because many of them are not found in the Spanish literature (important to the original publication of this work);[57] and second, because they help broaden a perhaps very narrow traditional conception of money, which could hinder the subsequent analysis of cryptocurrencies as just another form of money.

Figure 7. Seashell coin necklace presumably ancient and from New Guinea. Source: ebay.

In the Banks Islands, there was a highly developed currency and credit system.[58] As in Rossel, the coins were packets of seashell discs, but they were not very elaborate discs, nor of high quality, and they were brought from Rowa, other islands which, like the Banks, are in Vanuatu. As in Mauss's explanation, the circulation of money in Banks was also closely related to honor and, in this case, it happened within secret societies or men's clubs, the most important of which were called *Suqe*. Members had to pay in this currency to join and ascend the ranks of these clubs. The club then distributed this income among the members, prioritizing

[56] Ibid., 318.

[57] This reason of course does not apply to this English version, but it is left as a testimony that their translation into Spanish was an important part of the original work.

[58] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 53.

those of higher rank. Because of this, the wealthier members would get even richer by investing in a prominent position there and then collecting dividends from the new members. The most common way for poor men to obtain money was to make loans. These loans were usually made at a rate of 100% interest, so that when they were repaid, they would have double the money they lent. The borrower did not request these loans, but the lender could impose them, and there was a moral obligation to accept them. Mauss explained, "Indeed, Banks Islands appear to be a creditor's paradise."[59] The relationship between the name of these islands and this credit culture, whether it exists or is merely an ironic coincidence, is not explained by the authors in either the ethnography or the compilation. Regardless, not paying did not result in slavery as in North America. Yet, it did have other stipulated punishments: the creditor's family had the right to move into the debtor's house and live at his expense until he paid off his debt. To avoid this, they used to ask, this time, at will, for a second loan to pay off the first one, but this doubled the debt.

> As a rule no written documents change hands, but all credit business is transacted in public. A great deal of the time and energy of the population is expended in an eternal effort to obtain payment from one's debtors to be able to pay one's creditors. Owing the the [sic] fact that every debtor is due to repay twice the amount he borrows, the amount payable is liable to exceed the total amount of money available, in spite of the fact that new money is constantly produced.[60]

It is difficult to avoid seeing the parallel with the globalized financial world and consider how negligible technological change has been in achieving this result. Neither industrialization, wage labor, governments, banks, nor even writing seems necessary to bring a whole society to this situation of permanent debt—only a sort of pyramid scheme and the quest for prestige of those involved in it.

[59] Ibid., 55.
[60] Ibid.

Figure 8. Mokos from Alor.
Source: https://www.yukepo.com/hiburan/indonesiaku/moko-benda-purbakala-yang-dilestarikan-masyarakat-alor-ini-jadi-bukti-kalau-indonesia-keren/" Yukepo.

Similarly, a credit system was developed in Alor, Indonesia, using gongs and metal vessels called *moko*.[61] The division of labor was clear-cut: women did all the manual labor while men seemed exclusively dedicated to finance. Although other objects functioned as currency, such as pigs and arrows, the gongs and *mokos* were the most valued possessions. The *mokos* existed in various forms with different values, as did the coins of Rossel, and were not used directly in the exchange of goods, but had a fixed price in pigs and among the different classes of currency. "By far the most important part played by *mokos* and gongs is in the sphere of credit. The total circulation of *mokos* in Alor serves as a basis for an inverted pyramid of credit structure that is not unlike that of our modern communities. On Alor, wealth consists essentially of a series of outstanding credits, not of accumulated property,"[62] such as in the American potlach. This activity kept these men busy full time: they had to be on the lookout to collect what was owed to them, find ways to pay their creditors, delay payments, get money and lend it quickly so it would not be collected, go collect from a debtor who was simultaneously collecting a debt from a third party, and so forth. "The lack of standardized currencies, the contest devices and the chicanery associated with wealth, the difficulties attendant upon feasts, the competitive system in which only a fraction of the male population can be successful, all contribute to the frustrations and irritations of gaining prestige."[63]

Just as debts could drive a *kwakwaka' wakw* or *tinglit* into temporary slavery, Einzig finds examples in which slaves embodied money itself. In Ireland, during the 1st and 2nd centuries, a monetary unit, the kumal, existed, at least among the nobility who left written documents, representing a "slave girl or bondsmaid." There is not much information about it, only a few mentions in some epic poems of pre-Christian Ireland. It is presumed that by the second century, it became an abstract unit of measure of value

[61] Ibid., 84.
[62] Ibid., 86.
[63] Ibid.

but not a medium of exchange. This is perhaps the example that Jevons had cited, without having much information about it either. A similar example closer in time was in the Bagirmi region of equatorial Africa:

> Slaves played the part of the standard of value for big transactions. The unit was a slave of medium qualities and the value of better slaves was expressed in terms of this standard slave. Wealth was reckoned in terms of "heads". When, after a successful slave raid the number of slaves for sale was large, the effect was the same as of a sudden increase of the monetary circulation in civilized communities. The price of all goods, horses, arms, chains increased in terms of the slave currency.[64]

One of the most interesting and widely cited cases in the bibliography referring to the diversity of forms in which money or currency exists is that of the Yap Islands, in Micronesia. These coins, called *rai*, are stone discs brought from distant islands such as Guam, ranging in size from a plate to twice the size of an adult.[65] According to Einzig, these stones derive their value from three factors: scarcity, since they are not stones found naturally on the island; cost of production, since extracting and transporting them involves enormous labour and a tribute must be paid to the local sovereign to allow them to be extracted; and the risk involved in transporting them. Their antiquity does not affect their value, and there do not seem to be myths about their origin that give them a sacred character, unlike Rossel's money or the cases studied by Mauss. One of the peculiarities of these stones, especially the larger ones, is that they change ownership without being physically moved, much like real estate. Changes of ownership are publicly announced, but the owners' names (along with those who made and transported them) are also

Figure 9. *Rai* stones from Yap. Source: Amusing (The original source on Flickr didn't exist, but was identified as Zinnie).

[64] Ibid., 131.
[65] Ibid., 36.

inscribed on each *rai*, so everyone knows who they belong to, and stealing them is impossible.

All stones function as stores of value, but there are differences in how they function as a medium of exchange. Small coins circulate smoothly, but the larger ones rarely change hands. Yap people prefer to keep their savings in large stones rather than small ones. Besides that, the use of these stones as a medium of exchange has certain limits: it only works in internal trade, not on other islands; much of the exchange is done in the form of barter; already at the time it was documented, the paper money with which wages were paid had gained place (despite some resistance or lack of understanding of its value by the inhabitants of Yap) and it is reasonable to think that today it has totally or almost totally displaced it; and, in addition, other objects also fulfill the function of means of exchange, even abroad (tobacco, taro, pearl shells, carpets, turmeric dyes and coconuts). On the other hand, there is no record that prices were expressed in *rai*, so Einzig rules out its use as a unit of account; however, it is used as a measure for deferred payments, and loans are made with them.[66] The interest on these loans is not as high as in the cases mentioned above. It seems that only after a few months did interest begin to be charged on them, which was paid in other forms of currency, such as pearl shells. The *rai* stones are also used in political payments, such as buying the support of a tribe in an intertribal conflict.

As for the value of the stones, Einzig finds contradictions or abrupt variations in the reports of different scholars on the subject. This may be due to the time at which the documentation was made: if Kubary, in the 1880s, reported that the purchasing power of the *rai* was minimal, it was likely due to the hyperinflation caused by Captain O'Keefe during that decade, as well as the previous one. Regarding this, Ammous dedicates a chapter in *The Bitcoin Standard*,[67] and Einzig also mentions it.[68] Furness's work (1910) followed a re-appreciation of the currency. Museums during the 20th century had a challenging time buying some of these stones because of their high price: a 30cm stone cost $75 in 1944; a stone the size of an adult person was worth several villages and plantations; and a stone the size of two adult persons was priceless. The islands were occupied during World War II, and dollars were brought in, but *rai* still retained their

[66] Ibid., 39.
[67] Ammous, *The Bitcoin Standard.*
[68] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects.*

value and use to some extent, even though new specimens were no longer imported.

After the two empirical sections, the third and last part of Einzig's book corresponds to theoretical developments that the author carries out based on all the cases reviewed. I will not develop that section in detail in this part of this book since the structure and concepts developed there will be the framework with which I will analyze Bitcoin and cryptocurrencies in the second part of this book.

Instead, I will limit myself to skirting certain conclusions he reaches because they complement, to a great extent, the developments made concerning money within economic science. The first of these had already been pointed out by Mauss previously and is one of the first things a scholar of the subject encounters when looking at ethnographic cases:

> I realized the need for laying stress on the non-commercial origin of money and on the possibility of the existence of credit before money, of money before barter and of barter before private property or division of labour in the generally accepted sense of these terms.[69]

Going a little further than Marcel Mauss, who, although he had questioned Hildebrand's postulate of stages, had not abandoned the model of stepwise evolution per se, Einzig intuited that the process of evolution of this phenomenon can take different forms and is far from being understood in orderly stages.

> It does not seem to have occurred to dogmatic advocates of a narrow definition that the main difficulty which the monetary theorist has to face in defining modern money is how to include within the scope of his definition abstract instruments of credit which have come to play a monetary role.[70]

The influence of his observations will be explained in the second theoretical section.

[69] Ibid., xvi.
[70] Ibid., 316.

◆ 1944-1945 Primo Levi: Auschwitz Prisoners' Economy

This case is not documented by an ethnography but by the personal account of Primo Levi, who was a prisoner in Auschwitz between 1944 and 1945. One of his books is entitled *Se questo è un uomo [If This is a Man]* and is one of the most detailed accounts of daily life inside these forced labor and extermination facilities of the National Socialist regime.

In the book's introduction, the author says: "It was not written in order to formulate new accusations; it should be able, rather, to furnish documentation for a detached study of certain aspects of the human mind."[71] And further ahead: "We would also like to consider that the Lager was pre-eminently a gigantic biological and social experiment."[72] There are many aspects of the 'human mind' to which the author reflects, as well as many facets of daily life, which he relates. One of the central themes of the work, and referred to in its title, is the dehumanization of the prisoners and what life is like under almost total deprivation. Upon arrival, prisoners were stripped of all their possessions, including their clothes, and their heads were shaved. They had to shower, disinfect themselves, and were given identical shoes and clothes. They were given beds, food rations, and medical care to keep them alive, but if any injury or illness rendered someone useless for work, they were eliminated. This was an attempt to homogenize all prisoners and reduce them to mere instruments of labor. In this context of scarcity, a whole discipline of resource utilization and a system of exchange flourished among the prisoners.

> We have learnt that everything is useful: the wire to tie up our shoes, the rags to wrap around our feet, waste paper to (illegally) pad out our jacket against the cold. We have learnt, on the other hand, that everything can be stolen, in fact is automatically stolen as soon as attention is relaxed; and to avoid this, we had to learn the art of sleeping with our head on a bundle made up of our jacket and containing all our belongings, from the bowl to the shoes.[73]

[71] Primo Levi, *The Complete Works of Primo Levi* (Liveright Press, 2015) Preface; book "If This is a Man: translated by Stuart Woolf"; volume 1. This chapter was not present in the most widespread edition, so it had to be cited from a different source.

[72] Primo Levi, *If This is a Man* (Orion Press, 1959), 99.

[73] Ibid., 29.

Possessions were limited to what each could carry, and property to what each could defend. However, that did not impede trade, loans, currency, and even price fixing. Levi recounts an ordinary morning as follows:

> The entire hut shakes to its foundations, the lights are put on, everyone near me bustles around in a sudden frantic activity. They shake the blankets raising clouds of fetid dust, they dress with feverish hurry, they run outside into the freezing air half-dressed, they rush headlong towards the latrines and washrooms. Some, bestially, urinate while they run to save time, because within five minutes begins the distribution of bread, of bread - Brot - Broid - chleb - pain - lechem - kenyer, of the holy grey slab which seems gigantic in your neighbour's hand, and in your own hand so small as to make you cry. It is a daily hallucination to which in the end one becomes accustomed: but at the beginning it is so irresistible that many of us, after long discussions on our own open and constant misfortune and the shameless luck of others, finally exchange our ration, at which the illusion is renewed inverted, leaving everyone discontented and frustrated.
>
> Bread is also our only money: in the few minutes that elapse between its distribution and consumption, the Block resounds with claims, quarrels, and scuffles. It is the creditors of yesterday who are claiming payment in the brief moment when the debtor is solvent. After that, a relative quiet begins, and many take advantage to go to the latrines again to smoke half a cigarette or to the washrooms to wash themselves properly.[74]

Although he speaks of the illusion that one's ration of bread was minuscule and that of others large, it is understood that the ration of bread was a standardized value that served as a measure for everything that was exchanged, but not as a storage of value, given its limited durability.

> It is notorious that only the High Numbers keep their bread in their pockets;[75] none of us old ones are able to preserve our bread for an hour. Various theories circulate to justify this incapacity of ours: bread eaten a little at a time is not wholly assimilated; the nervous tension needed to preserve the bread without touching it when one is hungry is in the highest degree harmful and debilitating; bread which is turning stale soon loses its alimentary value, so that the sooner

[74] Ibid., 37.

[75] The high numbers represent the last prisoners to arrive, as they were numbered as they entered.

> it is eaten, the more nutritious it is; Alberto says that hunger and bread in one's pocket are terms of opposite sign which automatically cancel each other out and cannot exist in the same individual; and the majority affirm justly that, in the end, one's stomach is the securest safe against thefts and extortions.[76]

The bread ration, then, had first to overcome the stage of ingestion to begin to circulate. Only those who could make the sacrifice of not eating the already scarce food available to them could, in principle, use it for something else. However, there was even a physical place where prisoners were grouped together to trade:

> The Market is always very active. Although every exchange (in fact, every form of possession) is explicitly forbidden, and although frequent swoops of Kapos or Blockalteste send merchants, customers and the curious periodically flying, nevertheless, the northeast corner of the Lager (significantly the corner furthest from the SS huts) is permanently occupied by a tumultuous throng, in the open during the summer, in a wash-room during the winter, as soon as the squads return from work.
>
> Here scores of prisoners driven desperate by hunger prowl around, with lips half-open and eyes gleaming, lured by a deceptive instinct to where the merchandise shown makes the gnawing of their stomachs more acute and their salivation more assiduous. In the best of cases they possess a miserable half-ration of bread which, with painful effort, they have saved since the morning, in the senseless hope of a chance to make an advantageous bargain with some ingenuous person, unaware of the prices of the moment.[77]
>
> At the Market you can find specialists in kitchen thefts, their jackets swollen with strange bulges. While there is a virtually stable price for soup (half a ration of bread for two pints), the quotations for turnips, carrots, potatoes are extremely variable and depend greatly, among other factors, on the diligence and the corruptibility of the guards at the stores.[78]

Bread was, then, along with soup, the conventional, everyday food, but by no means the only one. The other foods were smuggled in, but one might ask why anyone would steal food to exchange it for food provided to them every day. The answer is that the trade went far beyond foodstuffs.

[76] Levi., *If This is a Man,* 84.
[77] Ibid., 88–89.
[78] Ibid., 90.

It is a question of stealing or receiving any of the various tools, utensils, materials, products, etc. with which we come in daily contact in Buna in the course of our work, of introducing them into the camp in the evening, of finding a customer and of effecting the exchange for bread or soup. This traffic is intense: for certain articles, although they are necessary for the normal life of the Lager, this method of theft in Buna is the only and regular way of provisioning. Typical are the instances of brooms, paint, electric wire, grease for shoes.[79]

It has to be realized that cloth is lacking in the Lager and is precious; and that our only way of acquiring a rag to blow our noses, or a pad for our shoes, is precisely that of cutting off the tail of a shirt at the time of the exchange. If the shirt has long sleeves, one cuts the sleeves; if not, one has to make do with a square from the bottom, or by unstitching one of the many patches. But in all cases a certain time is needed to get hold of needle and thread and to carry out the operation with some skill, so as not to leave the damage too obvious at the time of handing it in. The dirty, tattered washing is passed on, thrown together, to the tailor's workshop in the camp, where it is summarily pieced up, sent to the steam disinfection (not washed!) and is then re-distributed; hence the need to make the exchanges as unexpected as possibile [*sic*], so as to save the soiled washing from the above mutilations.[80]

Mahorca is a third-rate tobacco, crude and wooden, which is officially on sale at the canteen in one and a half ounce packets, in exchange for the prize-coupons that the Buna ought to distribute to the best workers. Such a distribution occurs irregularly, with great parsimony and open injustice, so that the greatest number of the coupons end up, either legitimately or through abuse of authority, in the hands of the Kapos and of the Prominents, nevertheless the prize-coupons still circulate on the market in the form of money, and their value changes in strict obedience to the laws of classical economics.[81]

Among the ordinary Haftlinge [prisoners] there are not many who search for Mahorca to smoke it personally; for the most part it leaves the camp and ends in the hands of the civilian workers of the Buna. The traffic is an instance of a kind of "kombinacja" frequently practised: the Haftling, somehow saving a ration of bread, invests

[79] Ibid., 95.
[80] Ibid., 87–88.
[81] Ibid., 90–91.

> it in Mahorca; he cautiously gets in touch with a civilian addict who acquires the Mahorca, paying in cash with a portion of bread greater than that initially invested. The Haftling eats the surplus, and puts back on the market the remaining ration. Speculations of this kind establish a tie between the internal economy of the Lager and the economic life of the outside world: the accidental failure of the distribution of tobacco among the civilian population of Cracow, overcoming the barrier of barbed wire which segregates us from human society, had an immediate repercussion in camp, provoking a notable rise in the quotation of Mahorca, and consequently of the prize-coupon.[82]
>
> The Haftling acquires in exchange for Mahorca or bread, or even obtains as a gift from a civilian, some abominable, ragged, dirty shred of a shirt, which must however have three holes suitable to fit more or less over the head and arms. So long as it only carries signs of wear, and not of artificially created mutilations, such an object, at the time of the Waschetauschen, is valid as a shirt and carries the right of an exchange.[83]

It follows from the above that, contrary to the original assertion that bread was the only currency, three currencies were circulated in Auschwitz: bread, tobacco, and bonds. Of these, two were commodity money (tobacco and bread), and the other (the bonds) was a money substitute deriving its value from its parity with a standard amount of one of the different currencies, tobacco. On the other hand, cloth served as a store of value but not as a medium of exchange. The most stable price seems to have been that of the bread ration, which was always delivered in the same quantity, while the voucher and tobacco were more susceptible to fluctuations:

> There have been periods in which the prize-coupon was worth one ration of bread, then one and a quarter, even one and a third; one day it was quoted at one and a half ration, but then the supply of Mahorca to the canteen failed, so that, lacking a coverage, the money collapsed at once to a quarter of a ration. Another boom period occurred for a singular reason: the arrival of a fresh contingent of robust Polish girls in place of the old inmates of the Frauenblock.[84] In fact, as the prizecoupon is valid for entry to the Frauenblock (for the criminals and the politicals; not for the Jews, who on the

[82] Ibid., 91–92.
[83] Ibid., 92.
[84] Literally "women's block," where female prisoners were sexually exploited.

> other hand, do not feel affected by this restriction), those interested actively and rapidly cornered the market: hence the revaluation, which, in any case, did not last long.[85]

Perhaps the only thing that inmates were not stripped of when they entered could be traded as well:

> There are some who do not hesitate to have the gold fillings of their teeth extracted to sell them in Buna for bread or tobacco. But the most common of cases is that such traffic takes place through an intermediary. A "high number," that is, a new arrival, only recently but sufficiently besotted by hunger and by the extreme tension of life in the camp, is noticed by a "low number" for the number of his gold teeth; the "low" offers the "high" three or four rations of bread to be paid in return for extraction. If the high number accepts, the low one pays, carries the gold to Buna, and if in contact with a civilian of trust, from whom he fears neither denunciation nor fraudulent dealing, he can make a gain of ten or even as much as twenty or more rations, which are paid to him gradually, one or two a day.[86]

On the other hand, the need and the minimal to no respect for individual property imposed a limit on the maximum volume of transactions:

> …the maximum total of any transaction negotiated within the camp is four rations of bread, because it would be practically impossible either to make contracts on credit, or to preserve a larger quantity of bread from the greed of others or one's own hunger.[87]

Finally, I quote a few more paragraphs on this peculiar economic system and how far beyond the prisoners it extended:

> … Those Häftlinge at Buna who have the chance to fill their bowl with grease or machine-oil (or anything else: any blackish and greasy substance is considered suitable for the purpose), on their return to the camp in the evening, make a systematic tour of the huts until they find a *Blockältester*[88] who has run out of the article and wants a fresh supply. In addition, every hut usually has its habitual supplier, who has been allotted a fixed daily recompense on condition that he provides the grease every time that the reserve is about to run out.

[85] Levi, *If This is a Man*, 91.
[86] Ibid., 93.
[87] Ibid.
[88] Literally "elder of the block", he oversaw organizing a block or barracks.

> Every evening, beside the doors of the *Tagesräume*[89] the groups of suppliers stand patiently around; on their feet for hours and hours in the rain or snow, they discuss excitedly matters relating to the fluctuation of prices and value of the prize-coupon. Every now and again one of them leaves the group, makes a quick visit to the Market, and returns with the latest news.[90]
>
> light-bulbs, ordinary or shaving-soap, files, pliers, sacks, nails; methylic alcohol is sold to make drinks; while petrol is useful for the rudimentary lighters, prodigies of the secret industry of the Lager craftsmen.
>
> In this complex network of thefts and counter-thefts, nourished by the silent hostility between the SS command and the civilian authorities of the Buna, Ka-Be[91] plays a part of prime importance. Ka-Be is the place of least resistance, where the regulations can most easily be avoided and the surveillance of the Kapos eluded. Everyone knows that it is the nurses themselves who send back on the market, at low prices, the clothes and shoes of the dead and of the selected who leave naked for Birkenau; it is the nurses and doctors who export the restricted sulphonamides to Buna, selling them to civilians for articles of food.
>
> The nurses also make huge profits from the trade in spoons. The Lager does not provide the new arrivals with spoons, although the semi-liquid soup cannot be consumed without them. The spoons are manufactured in Buna, secretly and in their spare moments, by Haftlinge who work as specialists in the iron and tin-smith Kommandos (…). Now it is a law that although one can enter Ka-Be with one's spoon, one cannot leave with it. At the moment of release, before the clothes are given, the healthy patient's spoon is confiscated by the nurses and placed on sale in the Market. Adding the spoons of the patients about to leave to those of the dead and selected, the nurses receive the gains of the sale of about fifty spoons every day.[92]
>
> In conclusion: theft in Buna, punished by the civil direction, is authorized and encouraged by the SS; theft in camp, severely repressed by the SS, is considered by the civilians as a normal exchange operation; theft among Haftlinge is generally punished, but the punishment strikes the thief and the victim with equal gravity.[93]

[89] The rooms where they slept.
[90] Levi, *If This is a Man*, 96.
[91] Nursery.
[92] Levi, *If This is a Man*, 96–97.
[93] Ibid., 98.

Levi's observations about economic life in Auschwitz confirm several assumptions of classical and orthodox theories of political economy. First, trade and currency do not need a community whose members are bound by solidarity and good faith to function. The climate in the Lager, Levi repeats several times, was one of perpetual mutual hostility and distrust; yet trade flowed and was sustained by trust in the means of payment as such, and in one's self-interest. However, as seen in other examples cited in this study, this does not mean that all economic systems operate in this manner, as those theories suggest. On the other hand, individualistic interpretations relate to what the author calls *the drowned and the saved*, a fierce competition for survival among all. This competition goes beyond the economic and, therefore, will not be dealt with here except in one aspect: no prisoner was considered rich in the Lager, since it was impossible to accumulate material goods.

On the other hand, they could accumulate prestige and become prominent, or Prominenz, individuals with benefits that most did not have. This prominence was not always achieved economically, but securing good deals and having the right business partners was one possible way to attain that status. But, unlike what Mauss observed, there was no mechanism by which this prominence was transferred or reified in the goods.

◆ 1969 Godelier: Production and Circulation of Salt Currency

Godelier, a French anthropologist from the historical materialism school, studied the Baruya ethnic group of New Guinea over three decades, from the 1960s to the 1980s. Although he inscribes himself within economic anthropology, he also studied other aspects of this ethnic group, including sexuality and power.[94] The book I cite, *Studies in Economic Anthropology*, is a compilation of papers on economic anthropology edited only in English. The book I cited in the Spanish version of this book was *Economía, Fetichismo y Religión en las Sociedades Primitivas* (Economy, Fetishism and Religion in Primitive Societies), a compilation of Godelier´s work, only

[94] Maurice Godelier, *The Making of Great Men: Male Domination and Power among the New Guinea Baruya* (Press Syndicate of the University of Cambridge, 1987).

edited in Spanish.[95] The original article on the salt currency was published in 1969 in the scientific journal *L'homme.*[96] In the prologue of the Spanish book, he describes the situation of these people in the following manner:

> …a society in the interior of New Guinea, where we carried out our apprenticeship in field practice between 1967 and 1969. For more than two years we lived and worked within this society, which had first seen a white person in 1951, and which was not under the control of the Australian Administration until 1960. In 1967, when we arrived, a colonial relationship, one might say in its incipient state, had just abolished the distance that had separated in time and space two extreme forms of the proteiform development of history. A classless society which had only just closed behind it the Neolithic door by procuring steel utensils from tribes in contact with whites, found itself confronted by foreigners who asserted and imposed their "right", in the name of the "superiority" of their own economic and social system, to "pacify" it militarily, to "civilize" it and then to leave it in the hands of anthropologists or other "men of science"; in short, the right to subject it to order for the benefit of a class society.[97]
>
> The Baruya claim to be descendants of the refugees of the Yoyué tribe living originally in the region of Menyarnya. They say they were obliged to flee their original territory after a conflict with other segments of their tribe who, in this instance, were allied with their enemies. We may estimate that this exodus took place about two centuries ago [1760] (…). At the beginning of the 20th century, they penetrated into the neighboring valley of Wonenara, and drove back its original inhabitants.[98]

From the above, it is evident that the Baruya had not been studied when Einzig compiled his work. Therefore, they were left out of it, even from his second edition of 1966, when Godelier was still studying them. However, Godelier notes that, like the cases compiled by Einzig, the salt was also in the process of losing its monetary quality:

[95] Maurice Godelier, Economía, Fetichismo y Religión en las Sociedades Primitivas, (Siglo, 1974)

[96] Maurice Godelier, "La «Monnaie de Sel» des Baruya de Nouvelle-Guinée," L'Homme 9, no. 2 (1969): 5–37.

[97] Godelier, *Economía, Fetichismo y Religión en las Sociedades Primitivas*, 15.

[98] Maurice Godelier, "'Salt Currency' and the Circulation of Commodities among the Baruya of New Guinea," Studies in Economic Anthropology, (American Anthropological Association, 1971): 54.

> The exchange of salt for bark capes remains the last solid part of the system but already the Baruya´s partners are more and more eager to be paid in shillings.
>
> (…) In 1967 it was almost too late to find traces of the stone adze exchanges and to revive the ghost of the Neolithic economy . Tomorrow, the baruya salt will be a useless item stored forever in the imaginary *Musée des Cultures Primitives*.[99]

This work is relevant because it is a late ethnography on currency, incorporating all the previous theoretical developments. The theoretical approach employed in this study is historical materialism, also known as Marxism, which, as I mentioned earlier, did not initially focus particularly on money as a subject of study in its original formulation.

Figure 10. Old salt bars in disuse stored in the hearths of the houses. Year 2010. Source: Allison Jablonko, Marek Jablonko, y Maurice Godelier, "Study Guide for the films TO FIND THE BARUYA STORY and HER NAME CAME ON ARROWS", chap. 10 The Baruya Forty Years Later.

The salt currency comes in the form of solid bars 60 to 72 cm long and 10 to 13 cm wide, and,[100] according to the author, the principle of its value responds to a nutritional need: sodium is a scarce component among the area's foods.[101] The Baruya perfected a process to extract salt from the ashes of a grass that they cut annually and then had to process. A specialist is in charge of this process, which is esoteric. Altogether, about twenty people participate in a salt production cycle.[102] The result is as follows:

> …fifteen bars usually come to 25 to 30 kilograms of salt. The oblong shape of the oven itself means that bars fabricated near the two ends are shorter than those hardened near the center. The Baruya classify the bars into three categories according to their size, each with its name, and each requiring its own exchange rate. Of the fifteen bars produced simul-

[99] Ibid., 65.
[100] Ibid., 56.
[101] Ibid., 55.
[102] Ibid., 56.

> taneously, four or five are small, four or five are medium-sized, and six are large.[103]

After being produced, these salt bars begin to circulate. In the production process, there is an agent the author calls the owner, the first proprietor of the total produced. Of the fifteen bars the owner has at the end of production, five and ten are distributed to his relatives and friends, who probably helped him with all the work, although the author does not clarify this. Of the remainder, the specialist is paid one or two for his services, leaving the owner with between three and nine bars for himself and his family. The exchange of salt bars among the Baruya themselves, he says, is limited, given that most goods circulate as reciprocal benefits, including salt itself. Where salt really acquires its currency status is in inter-tribal trade. Historically, the Baruya have developed salt production to obtain their subsistence goods and ceremonial objects, which they cannot procure in their territory.[104] This characteristic of social life and production challenges, above all, the concepts of surplus and subsistence economy. There is not a moment of production of subsistence goods first, and then a second moment of exchange of these essential goods for others of second necessity. Exchange is necessary for this society's subsistence; salt, being produced for exchange, is a commodity, merchandise, an object made for commerce.[105]

> [Its] use value (...) is that of a ritual item highly valuable because of its ideological and social meaning as well of its nutritional or dietary importance, its flavor and the difficulties of its production.[106]

On the other hand, exchange value seems to respond more to the principles of Menger's subjective or utility-value theory than to the labor-value theory of the classics. In the author's words:

> From our own observations, he will, during a trading session, use the first type of argument in order to play on his partner's emotions: "My children have nothing left to cover their backs with..., etc." Later, if the partner remains unmoved, he will bring work "in consideration". An informant told us one day: "When we are bargaining, work is the last motive put forward. Work is something

[103] Ibid.
[104] Ibid., 64.
[105] Ibid., 65.
[106] Ibid., 65–66.

> belonging to the past and almost forgotten. It is only remembered it the partner is exaggerating his demands."
>
> The balance of exchanges is thus primarily regulated by the volume of social necessities.
>
> (…) The exchange is fixed at a level which indicates both the need and the work (or the effort necessary to procure a resource), but work seems to play a secondary role: it only defined as a kind of minimum below which the rate of exchange should not go, whereas the need, the scarcity of the product, seems to define the maximum level it could reach.[107]

In any case, it remains to be established whether use value and needs are subjective, as theorists of subjective value state, or whether the biological processes from which they derive endow them with a certain degree of objectivity.

Although such bargaining may exist, it is common for prices to be established for each product and for both parties to know how much they will receive in exchange for what they give. However, these prices are not the same for all the tribes with which the Baruya exchange was made, but they have been agreed upon with each one and are therefore always different. Moreover, in terms of labor time, the Baruya received several times more than what they gave, which Godelier explains by saying that "salt is expensive because it is a 'luxury item' the production of which requires both technical and magical knowledge that the neighboring tribes do not possess."[108] Unlike other cases in Oceania where credit and loans were significant, they seemed to play a minimal role in the salt market. His example is the following: if a Baruya needed to buy a female pig, he would require four bars of salt, of which he would probably borrow two. To repay the loan, this person will give one offspring of that pig for each bar. Since the animal had cost him four bars, he would pay back four times as much to each creditor. A high rate, but one that nevertheless did not motivate the Baruya to develop a credit and capital system like that of the Banks or Rossel Islands.

[107] Ibid., 66–68.
[108] Ibid., 68.

Experimentation: Social Currencies

Second empirical section. The so-called social currencies are a medium of exchange that is characterized by being created as such on purpose (unlike the cases in the previous section, in which the medium of exchange arises beyond the conscious decision of its users) but not within a hierarchical social structure, i.e., not imposed by an authority, but by a collective agreement of the users. I decided to place these cases separately from the ethnographies in the previous chapter, as it will be seen that the actors who documented their experiences also have a fully active role in developing and using these currencies, as implied by the above definition. For this reason, it seems more appropriate to consider these cases as experiments, differentiated from the observations in the previous chapter (apart from the first case, that of the capuchins, which are experiments, but the experimenters are separate from the subjects with whom they experiment). As in the previous section, important theoretical conclusions are drawn from these experiments, and criticisms are made of some of the theories presented in the first section, while others are vindicated.

The specific bibliography of this section consists of four volumes: (1 and 2) the studies on alternative currencies and parallel economies that emerged during the economic crisis of the years 2001 and 2002 in Argentina, carried out by a team from the National University of Luján;[1] (3) the book by Georgina Gómez, from the Erasmus University Rotterdam, on the *Red Global de Trueque* (Global Barter Network);[2] (4) and Yasuyuki Hirota's

[1] Ricardo Orzi, R. Borrello and A. Plasencia, *Moneda Social y Mercados Solidarios I: Potencial Emancipador y Pedagógico de los Sistemas Monetarios Alternativos* (2007); Ricardo Orzi, Ricardo Borrello, Carla Costa, et al., *Moneda Social y Mercados Solidarios II: La Moneda Social Como Lazo Social* (2012).

[2] Georgina M. Gómez, *Argentina's Parallel Currency: The Economy of the Poor,* (Picketing & Chatto Ltd, 2009).

PhD thesis,[3] by the University of Valencia. This section's criterion for selecting examples addresses the broadest possible diversity of ways social currencies can function. None of these books, to my knowledge, is available in a different language besides the one of the versions cited here.

[3]Yasuyuki Hirota, *Monedas Sociales y Complementarias (MSCs): Sus Valores Socioeconómicos para Distintos Stakeholders* (Tesis de doctorado, Institut Universitari d'Investigació en Economia Social, Cooperativisme i Emprenedoria [IUDESCOOP] 2017).

◆ Classification Schemes

In the fourth chapter of his thesis, Hirota classifies social and complementary currencies (SCMs) into several types according to their backing.

Table 3: Cuadro de clasificación de MSC de Hirota.[4]

Backup Type	**Subcategory**	**Examples**
Goods or services	Legal tender backup	Chiemgauer, SOL-Violette, Banco Palmas
	Other goods and services backup	Banco de horas comunitario, Terra
	Tax payment	National oxidizable currency (Gesell, 1916), currency by the Monetary Creation Committee (Jackson and Dyson, 2012).
Transaction	Mutual credit	LETS (CES), Trocobuy
Debt	Issuance as credit	Euro, WIR, Chiemgauer
None	Fiat	Ithaca Hours, Club de trueque

Similarly, the authors of *Moneda Social y Mercados Solidarios II* (Social Currency and Solidarity Markets II) classify the cases they studied (the same as in the first volume) according to the mechanism by which social money is issued. They develop an analysis of the concepts of money and currency using these empirical cases. They seek to distance themselves from the orthodox currents of economics for ideological reasons (to oppose theories that justify the free market) and instead adopt post-Keynesian conceptual frameworks (associated with an interventionist ideology):[5] chartalism, explained previously in this thesis; and endogenism, which "understands that money is a product of the banking system."[6] In Mises's typology, social currencies can be categorized into *money certificates, fiat money,* and *credit money.* The post-Keynesian theories mentioned above claim to demonstrate a unique origin of money, both historically and logically. Still, the evidence of the ethnographic and historical studies mentioned in the previous chapter of this work does not support this assertion.

[4] Ibid., 115.

[5] Orzi, Borrello, Costa, et al., *Moneda Social y Mercados Solidarios II: La Moneda Social Como Lazo Social*, 29–80.

[6] Ibid., 59.

Since this work has already dealt with the chartalist theory, I will devote a few paragraphs to the endogenist theory mentioned in that volume.

> Business spending generates the income of the system's participants, which will lead to demand for the goods produced by them; finally, the flow of income will allow the repayment of loans. Banks make loans to the extent that they can rely on the solvency of their customers and, in case of financial difficulties, the Central Bank would cover them to avoid the collapse of the system.
>
> Therefore, the money is issued by the banking system and the State only plays a passive role following what happens in the loan market.[7]

The endogenous hypothesis is thus presented in a functional or logical dimension. The starting point of an economy is the loan, the financial capital, which then becomes productive capital. This is contrary to the explanation of orthodox theories, which view the monetary economy as a by-product or as built upon the real economy.

But it does not stop there, from a historical perspective, it constructs a whole myth about the origin of money from credit:

> In primitive communities, human beings had social obligations linked to the debt for life to ancestors and deities. These payments implied a "hierarchy of value," that is, they depended on an individual's position and status in society; hierarchies that were historically established long before the emergence of the market.
>
> Human sacrifices to pacify the gods were an integral part of many primitive communities, being complemented by the donation of valuable gifts to the priests who were to mediate between society and the cosmos.
>
> (...) In short, contrary to the neoclassical interpretation, society was a moral community before it was a market, and money did not originate to facilitate transactions, but as a unit of account to establish compensatory payments for damages caused to other people or to the community.[8]

Although the latter assertion is quite accurate according to ethnographic and historical evidence, admitting such an evolution as the only possible one is problematic. The etymological evidence quoted in support of this hypothesis is exclusively from Indo-European and rather Anglo-Saxon languages, so it is not readily applicable to all languages. However,

[7] Ibid., 60.
[8] Ibid., 70–71.

as a theory I will review in the next chapter will explain, the main idea that money is a product of credit and not vice versa seems to be a key to understanding it, even if equating it with a unit of account is also a mistake.

Table 4: Equivalence of the MSC classifications discussed and the Mises money classification mentioned

Orzi	Hirota	Mises
Endogenism	Mutual credit	Credit-money
	Issuance as credit	
	Goods/services	Money certificates
Chartalism	Legal tender	
	Fiat	Fiat money
	Taxes	

Gómez's book provides an in-depth examination of the development of the Global Barter Network. In the following chapter of this work, I will present a broad outline of this study. From the first volume of *Moneda Social y Mercados Solidarios*, I will take the second section, which presents initiatives of this type organized throughout Argentina. I am more interested in concrete cases than this volume's theoretical part. If I were to address that segment here, I would reiterate the book's first chapter, which already refers to, or at least alludes to, the same hypotheses and theories. However, I am interested in highlighting from these experiences how the control mechanisms worked in the payment system and the problems these networks faced. Nor is it the aim of this section to cover all the categories presented, which is done in Hirota's work, but to analyze different cases presented in these volumes.

◆ The Red Global de Trueque (Endogenist, Issuance as Credit)

This network consisted of several *Clubes de Trueque* (barter clubs, CTs) throughout the provinces of Buenos Aires and Santa Fe, but it originated with a single club in the town of Quilmes in 1995. It originated when two environmentalist initiatives came together: the *Programa de autosuficiencia regional* (Regional Self-Sufficiency Program, PAR) and the *Red Profesional* (Professional Network, RP).[9] The former aimed to teach urban agriculture and promote self-sufficiency in food production, while the latter was a group of professionals who exchanged information on employment opportunities. Both projects aimed to help the so-called new poor, the middle class that had lost its position due to the economic imbalances of those years. The CT was formed because "They wanted production, trade and consumption to occur within a local exchange network where all the participants would contribute and benefit from each other's capabilities and resources."[10] The key figures of this club, and then of the network, were Carlos de Sanzo, psychologist and environmentalist, Ruben Ravera, museum director, and Horacio Covas, chemist, who all three had a previous socialist militancy.

The club began with weekly meetings at de Sanzo's residence:

> Participants offered and accepted home-made foods, handmade toiletries, organically grown vegetables, and handicrafts.[11]
>
> By around March 1995, after six months of experimentation with about twenty-five participants meeting every Saturday, the group developed an exchange system they found to be effective and practical. Participants came into the garage and placed their products on a table. The value was calculated at the formal market prices and was recorded on individual cards carried by the participants and on a computer worksheet. When the value of everyone's products had been recorded, all the participants went out and then returned as consumers to choose their 'purchases'. The value of these was deducted from the amount on their cards. (...) When they left, their 'purchase' was entered as a debit on both the card and the computer worksheet. In this way, the balance roughly returned to zero every

[9] Gómez, *Argentina's Parallel Currency: The Economy of the Poor*, 69.
[10] Ibid., 71.
[11] Ibid.

> week. (…) It was multireciprocal, so two individuals did not need to barter with each other directly. In the innovation loop, the payment system was a novelty. Transactions were recorded as credits and debits in a computer system designed by Horacio Covas. It was an ingenious transformation to standard market exchange, a club market with its own rules.[12]
>
> It soon became clear that bookkeeping based on individual cards and computer records was a poor mechanism. As the membership reached sixty, De Sanzo and Covas felt that entering Saturday's transactions into the file the following day was too burdensome. Besides, Covas did not like the centralization inherent in the system.[13]

The club organizers could have kept the number of members at a maximum, but they preferred to expand the club as much as possible and had to modify the exchange scheme. Two more clubs were formed nearby, and the system of a centralized spreadsheet was no longer sustainable. The solution that seemed most appropriate to them was to print banknotes, which they called *credits*.

> They initially experimented with a means of payment that could only be used once. They called it 'unidirectional money'. Those who paid with that money as well as those who received it had to sign each note and at the end of the day all the vouchers were submitted for a sort of clearing-house operation.[14]

But that did not work out well, so each club began creating its own bills or 'exchange coupons'. The unit of account was the peso, which was then equal to the U.S. dollar. This system helped the exchange in the clubs:

> …participants did not perceive the first vouchers as money. Trade was already happening with verbal promises to pay each other. When scrip appeared, it monetized those promises, eliminated the work of keeping records and removed the market-makers from the centre.[15]

Gómez offers a reflection on the differences between the two accounting systems:

> At an aggregate level, the card accountancy system used in the beginning was different from the use of a currency. Monetary creation

[12] Ibid., 72.
[13] Ibid., 74.
[14] Ibid., 76.
[15] Ibid., 78.

> would follow exactly at all times the rhythm of transactions and was not limited to an amount fixed *a priori*. In this sense it was an endogenous monetary system as described in the post-Keynesian literature. It regulated itself autonomously to the amounts traded, so monetary inflation was not possible. Later, the system with surrogate currency enabled saving for the next meeting, so production was equal to consumption only in the medium term. It was still an endogenous monetary system, but it regulated itself to the number of users of the currency, not the amounts traded.[16]

The second stage of the RGT's history occurred between 1996 and 2002, encompassing the growth process that transformed it into a network of clubs and the largest complementary economy among all those that have existed to date. This involved transforming the exchange from a personal to an impersonal one.

Initially, growth was gradual, as information spread among acquaintances and relatives. New members were always brought in by someone who was already participating. Some people traveled further and further to reach the club in Bernal, so the organizers decided to promote the creation of other clubs that were more accessible to these individuals. They also began to appear in the press and to teach workshops on how to create more clubs. They began to call the clubs 'nodes' and the whole group of clubs a 'network', terms taken, according to the organizers, from computer science,[17] which in turn was derived from mathematics, specifically from graph theory proposed first by Euler.[18] Credits were issued in increments of twenty per new participant and were to be returned upon leaving the club.

When the mainstream and mass media turned their attention to these clubs, the organizers began to receive many inquiries about how to participate and start CTs in various locations.

> As a result of the media exposure, the scheme grew to the limits of personal exchange regulation. A trust relationship with the new coordinators had still to be built during the initial meetings, which

[16] Ibid., 78–79.

[17] Ibid., 89.

[18] Leonhard Euler, "Solutio Problematis ad Geometriam Situs Pertinentis," *Commentarii Academiae Scientiarum Petropolitanae* 8 (1741): 128–40. On the subsequent development of the theory and the coining of these terms, see Carlos Reynoso, *Redes Sociales y Complejidad: Modelos Interdisciplinarios en la Gestión Sostenible de la Sociedad y la Cultura* (Complejidad Humana, 2011): 26–30.

> meant a further step towards impersonal exchange. The PAR then started offering training courses to prospective coordinators, introducing them to the principles of the scheme and its environmentalist-communitarian ideology, and basically getting to know them.[19]

Thanks to this exhibition, they were contacted by an NGO called *Red de Intercambio de Saberes y Cibernética Social* (Knowledge and Social Cybernetics Exchange Network). This NGO was headed by Heloisa Primavera and Carlos del Valle, well-known activists in the field of complementary and solidarity economies' activists, and university professors.[20] As a result, they helped the network by giving it academic support. From that moment on, the network began to be called the *Red Global de Trueque Solidario* (Global Solidarity Barter Network).

> By 1997 transparent management of the créditos was becoming a pressing issue. Not all participants and nodes accepted the vouchers of all the others and it was broadly left to individual discretion. (…) The issue came to a head when the network experienced its first case of forgery of scrip in the city of San Pedro. (…) Clearly, using a non-state currency beyond the realm of personal exchange was going to require regulation of impersonal exchange institutions.[21]
>
> The government of Buenos Aires city then came into the picture, supporting the First Workshop of Multi-reciprocal Exchange. The event was attended by 1,300 and formally introduced the *Trueque* to Argentine society. It was also the first gathering of all CT, many of which did not know the others existed. The workshop participants recognized the advantages of functioning as an integrated network in terms of synergies, division of labour, and so forth, but many also resented that *PAR* was more powerful than the others (...). The event represented a new step towards building institutions of impersonal exchange. It inaugurated the practice of meeting regularly, though in the beginning informally and without a structure.[22]
>
> The institutions of impersonal exchange were finally formulated. Every CT was to hold regular general meetings to choose the coordinator, among other tasks. Nodes were integrated into regions, with a single voucher and common rules of issuance and control. Coordinators were representatives to regional committees, which were responsible for controlling the issuance and distribution of créditos.

[19] Gómez, *Argentina's Parallel Currency: The Economy of the Poor*, 90.
[20] "Heloisa Primavera," The Social Solidarity Economy Resource Website.
[21] Gómez, Argentina's Parallel Currency: The Economy of the Poor, 92.
[22] Ibid., 92–93.

> The national Inter-zone Coordinators' Committee (IZ) was created. The IZ came the highest body in the network and met once a month with two representatives of each area committee across the country. It had a variety of functions (discussing problems, proposing strategies and projects, sharing experiences, and preparing training materials for new coordinators and prosumers). The crucial function was to control the *créditos* issued and distributed in each region, so all vouchers would be acceptable across the country.[23]

Table 5: RGT organization.[24]

Types of agent	**Organizations where they participate**	**Level of operation**	**Types of relation**
Regional representatives	Inter-zone committees	National	Impersonal ties
Coordinators	Regional committees	Regional	Weak personal ties
Prosumers	*Club de trueque*	Local	Strong personal ties

There were political disagreements between PAR and the so-called anti-PAR front: the anti-PAR agreed with this bottom-up organization, while for PAR, bureaucratization and politicization brought inefficiency and more work. PAR conceived barter as a market within the market , but the anti-PAR went further and wanted to turn it into a state within it, in a radical economic-political change.[25]

> …while the institutional design of the Trueque responded at times to the intention of improving efficiency and scaling up from personal to impersonal exchange, this was not a constant over time or for all agents. It never ceased to be a factor driving institutional design, but power struggles and social relations between leaders were embedded in the organizational process and eventually explain much of the final outcome.[26]

In 1999, PAR decided to break away from IZ and organize the entire network in its own way, with what they called 'social franchising'. An aspiring organizer could purchase the CT kit for $2 and establish their local node, integrating it into the RGT with vouchers issued by PAR. PAR

[23] Ibid., 94.
[24] Ibid.
[25] Ibid., 95.
[26] Ibid., 96.

became a central bank for the network, overseeing all monetary policy, and barter became a purchasable commodity rather than a collaborative construct. The franchise was more successful at the club level, and its nodes grew larger than the non-integrated ones, beginning to compete aggressively with them. By 2002, they had 3500 nodes.[27] The anti-PAR accused the PAR leadership of having a non-transparent management of credit issuance. In 2000, PAR rebranded its network as the RGT and formally abandoned the IZ. Another group followed suit and formed the *Red de Trueque Zona Oeste* (West Zone Barter Network, ZO). ZO and PAR each accepted the credits of the other network. The rest of the IZ rebranded itself as *Red de Trueque Solidario* (Solidarity Barter Network, RTS).

Parallel to this dissolution, the popularity and notoriety of these markets grew rapidly. "A handful of municipalities actively helped the scheme by providing buildings or vehicles to transport goods. The relation with the central government was different, more of tolerance than acceptance."[28]

> With the increasing scale of the nodes, diversity of supply expanded until there were few goods that could not be obtained in créditos. Members became incredibly creative in widening the scope of products offered: from vegetables and fruits to clothing and shoes, books and CDs, home-made toiletries, furniture, and electronics. Some services, such as haircuts, manicures, wedding parties and Tarot fortune-telling, were offered on the market premises. Others, such as legal counselling, car insurance, taxi and courier transport, holiday packages, and education and training, were advertised on bulletin boards. Even plots of land in the countryside and livestock were offered for sale in créditos.[29]

The country was experiencing one of its worst economic crises at the time, which led more people to visit these markets in search of food, and the available supply was insufficient to meet the high demand. This increased prices and inflation of credits, which in 2001 lost parity with the peso. The PAR still had no organized control over the printing of vouchers, and in 2002, a large-scale counterfeiting of vouchers finally broke the RGT. It was never entirely clear how or why this counterfeiting was organized, but several testimonies exist:

[27] Ibid., 99.
[28] Ibid., 114.
[29] Ibid., 115.

> You could see people selling packs of forged vouchers near the entrance of almost every large node. They were even available in the nearby kiosks. We wondered many times who has the capacity to do that. Printing costs money and these criminals must be making money. For me, the politicians were behind it because they didn't like the *Trueque*.
>
> (…) The Trueque, they say, was no longer tolerable for Peronist leaders, who were unhappy that the clientele of their networks had an alternative source of income with elections coming up (P. North, 2005). Groups connected to the Peronist party also opened nodes specifically for their political clientele.[30]
>
> Apparently, they paid 800 pesos a day to 50 printers to counterfeit our vouchers. This was a centralized, organized action. They put 500 million credits in our market, and this led to very high inflation. It cost them more to print them than what the credits themselves are worth. This means that the objective is to destroy our system and not to make a business out of counterfeiting.[31]
>
> …they did everything to the guy: inflation attack (they falsified a lot of tickets), media and judicial persecution; and they threatened him and all his family.[32]

Whoever did this, and whatever their objective, the result is that the RGT collapsed due to the lack of confidence that this incident brought about. Simultaneously, there began to be social plans from the government, and many people began to receive income directly in pesos. In 2003, the regular economy began to grow, and many people secured formal or informal jobs, earning an income in legal tender. Other markets, similar to this one but on a smaller scale, continued to function and demonstrated greater resilience.

◆ Red Mar y Sierra (Fiat Chartal)

Carlos W. Pérez Lora's presentation in the Orzi and Borrello volume explains how an extensive network of barter markets, *Red Mar y Sierra*,

[30] Ibid., 117.

[31] "Denuncian un Complot para Destruir el Sistema del Trueque," Clarín (2002).

[32] Personal communication. Refers to one of the complainants of the above-mentioned note.

operated.[33] This network also invented its own currency to enable trade in the 1990s and 2000s, when many people were excluded from the formal labor system. In 2002, the network covered sixteen municipalities in the Buenos Aires province, with 105 nodes and 46,000 members. It was part of the RTS, mentioned in the previous chapter.

> …We considered barter to be a complementary economy, because it could never have been an alternative economy, especially in the way it was originally conceived. For those who did not have at least a Plan Jefas y Jefes or a Plan Trabajar (welfare programs) at that time, the system did not work, because there was always a need for a member of the family to have some kind of income in cash.[34]

This author states that the credits circulating in the barter markets, serving as social currency, had to maintain parity with the peso to establish a reference value. That, in addition, "it was controlled by all and used by all."[35] However, this control was fundamental for this system, but it demanded a significant investment of work. Lora explains in detail the functioning of the IZ mentioned in the previous chapter:

> the issue with social currency is that, in order to be social, everything had to pass through control and that this control could not be carried out by two or three, but that we had to control each other collectively, that is to say, social currency because it had a social control. And that is how a whole organic structure was set up, where the Coordinators were elected by the Assembly, where the Account Reviewers were elected, apart from the Coordinators, with the same system, where monthly balance sheets were prepared by each Node, which were elaborated by the Coordinators and reviewed by the Account Reviewers of that Node. Once approved, the balance sheet was again reviewed by an Account Reviewer of another Node to avoid possible collusion between a Coordinator and an Account Reviewer of the same Node. The balance sheets were then posted on the Node's bulletin boards so that all members would know what was being done with their credits.
>
> These balance sheets were made in each Node, then balance sheets were made for all the internal zones that made up the regional network, and a final balance sheet was made for the region. This final

[33] Orzi, Borrello, Costa, et al., *Moneda Social y Mercados Solidarios II: La Moneda Social Como Lazo Social*, 62.
[34] Ibid., 64.
[35] Ibid., 66.

> balance was presented at the monthly meeting of the IZ of the RTS, where it was reviewed by coordinators from other networks in the country.[36]

There was a complex system of peer verification to avoid delegating all trust to a central authority, but this required numerous instances, extensive work, and bureaucratic organization. The currency was equivalent to one peso, the legal tender, but it did not have a backing; that is to say, there were no reserves in pesos for the same number of coins issued. However, the members agreed to accept it at that rate. The circulating currency was controlled, increased, or decreased as necessary, and maintaining the peg was fundamental for them.[37] He goes on to explain:

> ...we used to say that we were too democratic because everything was done very slowly but, we insisted, we were seeking to tutor people and as this was growing and this structure was in place to support it, this allowed us, in our case, to withstand the shock.[38]
>
> But on the one hand, what we are looking for is that others to become engaged too, because otherwise we are always the same faces, and this would be a sign that the work we did was not so good.
>
> That on the one hand. On the other, we must consider that, not in Mar del Plata but in other cities of the province of Buenos Aires, one thing that also affected bartering was the welfare income plans. This greatly affected barter where there was clientelism. Because where there was clientelism, in a family with four members there were four plans. If you have a basic salary of $600, for what are you going to barter? This made bartering disappear in many towns in the interior of the province. Where it was not controlled. In other places, where it was controlled or not so discretionary, many people used part of what they were given by the plan to convert it into raw materials and produce to sell in barter.[39]
>
> We were two psychologists, twenty-five housewives, two plumbers, one carpenter. The only professionals were my wife and I, and we are psychologists. And we did it all without theory, and then we saw how it was misrepresented. Then came what we call the "rectal" franchise, the famous conversion of the barter into a McDonald's, and that is when it all rotted away.[40]

[36] Ibid., 65.
[37] Ibid., 66.
[38] Ibid., 90.
[39] Ibid., 94.
[40] Ibid., 91.

> I believe that we must vindicate within the node what "small is beautiful" meant, the face-to-face link.[41]

◆ Venado Tuerto (Chartal Shrinking)

Daniel Ilari, in the following chapter of that volume, presents a similar problem in the Venado Tuerto experience, of which he is or was the coordinator, with a much smaller number of participants:

> At the beginning we had a book where everyone wrote down the exchanges, which was possible up to about one hundred participants; when we reached one hundred participants it became very difficult to control all the exchanges, and it took so much time that we decided to switch to the "*billetito*" (little ticket).[42]

That is to say, the means of record-keeping was initially an annotation kept by each participant that had to be verified. Since this verification was too costly, due to the large number of participants and the high volume of transactions (which likely grew exponentially), they had to introduce a means of exchange between the goods that circulated, a currency. This currency "had to have two fundamental characteristics: the first was that it should lose value over time, which was Gesell's original idea; the second was that the medium should be maintained locally."[43] The shrinking mechanism, devised by Silvio Gesell in his work *Die natürliche Wirtschaftsordnung durch Freiland und Freigeld* (The natural economic order through free land and money),[44] and applied in this small-scale market, works like this: "the 'points', are losing value over time, every four months they expire, and the people who still have them must go and exchange them, losing 5% value for keeping them in their possession."[45] At first sight, this would not seem to differ much from the inflationary system with which legal tender currencies operate. However, there is a significant difference: the legal tender currency constantly increases its circulating value, and the loss of its purchasing power is a consequence (implicit and often disguised) of this and of other macroeconomic variables; on the other hand, in the

[41] Ibid., 95.
[42] Ibid., 68.
[43] Ibid., 70.
[44] Silvio Gesell, *The Natural Economic Order* (Peter Owen, 1958)
[45] Orzi, Borrello and Plasencia, *Moneda Social y Mercados Solidarios I: Potencial Emancipador y Pedagógico de los Sistemas Monetarios Alternativos*, 70.

oxidizable currency the loss of purchasing power and its expiration date are explicit rules. At the same time, the currency in circulation is adjusted to match the quantity of products in circulation, which implies that prices remain stable.[46]

> It is especially important to deal with each other because, in my region, I would say that half of the barter clubs that closed were because they ended up fighting and there was no way to continue.[47]

This problem is particularly critical for these economies due to three key factors: first, because they are firmly rooted in local communities and characterized by face-to-face relations among the same people; second, because they lack coercive means of cohesion; and third, because they are integrated into a larger economic system. On the other hand, state-capitalist economies maintain economic and personal relations as separate spheres, compelling citizens to accept legal tender; therefore, the breakdown of emotional ties between participants does not affect economic relations. This motivated the Venado Tuerto club to invest money in keeping emotional relationships on good terms:

> ...people who want to be trained are paid. This is contrary to the capitalist system in which you pay for the course, but here you are paid to attend the course. Fundamentally we implement it when it is a topic that has to do with human relations or the capacity of people to relate to each other.[48]

◆ Poriajhú (Debt Endogenist)

This market began operating in 1992 as a cultural center or workshop to solve the problem of school dropouts. In 2000, they joined the Global Barter Network, which collapsed in the following years. In 2006, they restarted their solidarity market with their own currency. This market is supplied with products from enterprises founded with credit in legal currency, provided by their microcredit system, *Banquitos Populares de la Buena Fe* [Popular Banks of Good Faith].[49] "Today [2012] we are shaped in several areas: education, solidarity economy, art, and communication. The

[46] Ibid., 71.
[47] Ibid., 72.
[48] Ibid.
[49] Ibid., 74.

four areas crossed by popular education."[50] The emphasis on education stems from the fact that "Poriajhú's objective is the construction of a true political community..."[51]

Currency, just another tool used for this purpose, is issued as credit to new market participants:

> ...barter participants receive the means of payment before participating in any transaction. Thus, the authority, based on a hierarchical principle, allows participation in the barter, and its participants contract a debt with the collective. This point facilitates the construction of authority beyond private interests.[52]

In addition, it promotes the cohesion of the trading parties:

> A great strength of barter is the direct contact between the producer and the consumer and that in this relationship everyone is a prosumer.[53]

This has allowed it to be highly resilient, as it...

> ...has been able to maintain parity between the peso and credit for all goods because credit enjoys important levels of ethical trust, unlike what happens in [a similar market in] Rosario; that is, parity is not questioned because it enjoys an ethical foundation.[54]

To maintain this dynamic, it is necessary, and for them desirable, to prevent the number of members from growing too much, as shown in this testimony:

> And when this boom [of 2001 and 2002] ended, what happened to us, ahhh! (Long sigh and slump of shoulders). When we went back to being the same as we were before, we said "this is the barter", because the other was a whole structure in which the barter was lost. You got lost in anonymity. We needed to recover the other, the other as a person, which is what constitutes us.
>
> (...) Then, afterwards, we felt great relief and we consider that period as possibly not repeatable and not recommendable for anyone,

[50] Ibid., 78.

[51] Orzi, Borrello, Costa, et al., *Moneda Social y Mercados Solidarios II: La Moneda Social Como Lazo Social*, 226.

[52] Ibid., 229.

[53] Orzi, Borrello and Plasencia, *Moneda Social y Mercados Solidarios I: Potencial Emancipador y Pedagógico de los Sistemas Monetarios Alternativos*, 78.

[54] Orzi, Borrello, Costa, et al., *Moneda Social y Mercados Solidarios II: La Moneda Social Como Lazo Social*, 225.

> because we believe that these spaces work. Maybe it is not necessary to be hermetically closed, but that there are clear rules of entry and exit, that diversity is respected. But what we will never recommend, nor encourage, nor participate in again, is such a massive phenomenon.[55]

Hadrien Saiag, in the second volume, contrasts the Poriajhú market with that of Rosario, and on this foundation, reflects on the role of currency in structuring social relations.[56] Its main objective is to refute the "instrumental" approach, according to which currency is a means of exchange that is neutral to the real economy. In the Rosario market, participants deliver goods to the market to obtain credits. These are credits from the market to them, which makes them creditors of the market. This results in the reproduction of the inequalities of the formal market, as privileged actors can move in both currencies.

> To obtain the means of payment (goods used as means of payment and paper currency), participants must deliver goods or pesos (because, as mentioned above, eight thousand credits can be obtained in exchange for ten pesos). This makes the group indebted to its members, which, in turn, fosters an atomic vision of the collective, making it strongly prone to being instrumentalized by its members. As a result, it is much more difficult for the group to constitute itself as such beyond its various private interests.[57]

In Poriajhú, on the other hand, credit is given to participants upon entering the market, so everyone enters with debt. This, coupled with a stronger form of authority, fosters greater cohesion and transforms it into a genuine movement for social change, engaging the actors more profoundly.

◆ Cosettini Timebank (Tax Endogenist)

The last case presented is that of a school cooperative and hour bank in Capilla del Monte, Córdoba. The cooperative was founded to provide education to families without access to it, and the time bank served as

[55] Orzi, Borrello and Plasencia, *Moneda Social y Mercados Solidarios I: Potencial Emancipador y Pedagógico de los Sistemas Monetarios Alternativos*, 92.

[56] Orzi, Costa, Herrera, et al., *Moneda Social y Mercados Solidarios II: La Moneda Social Como Lazo Social*, 205–36.

[57] Ibid., 229.

a system to manage work and keep the school running. According to the presentation by Marcelo Caldano, coordinator of this project, the currency was created as follows:

> ...We had a problem of inequality (because the poorest were the ones who worked the most because they were the ones who had more time for all the things that were needed to support the school), so we decided to log the hours worked by each of the families and we agreed on three pesos ($3-) an hour.
>
> Then we began to register the hours worked that were going to be compensated with products and services.[58]

This system allows them to make visible or quantify the capital of a large number of workers who had been excluded from the formal economic system.

> Capital is that part of the assets that sets in motion a surplus production and increases productivity.
>
> (...) What are the assets of the marginalized?
>
> - Their labour force
> - Their knowledge and skills
> - Their work capacities
>
> (...)
>
> What is it that produces surplus production? The commitment to the common good (...)
>
> How do we make the capital visible? By means of solidarity contracts, the "solidarity check", we make the workforce committed to the common good visible and accountable. (...)
>
> By means of the Institutional Currency, we make this capital fungible, with which we develop the activities of the Social Organization (...).
>
> What is the backing of the institutional currency?
>
> - The work commitments signed by the members
> - Donations in kind
> - The products of the micro-enterprises associated with the Bank: honey, flour, eggs, Internet

[58] Orzi, Borrello and Plasencia, Moneda Social y Mercados Solidarios I: Potencial Emancipador y Pedagógico de los Sistemas Monetarios Alternativos, 83.

- The productive capacity of the partners (institutional market, listings)
- Educational services: university classroom, complementary education.[59]

They also reached an agreement with the municipality to pay taxes with their points:

> …the municipality collects 30% of the municipal taxes in points and this is exclusively dedicated to the social area (...). And we have been following the Electric Cooperative for some time to get them to accept points, we must go in on the side that it is convenient for them, but if people could pay all services in points, the currency becomes much stronger.[60]
>
> **Carlos [Lora, Red Mar y Sierra presenter]:** It is paradoxical: they are looking for it to be approved and with us it was the other way around, it was offered to us by several municipalities, and we refused, because it was precisely to give a value to that bill that we did not acknowledge... What we did want, and this was approved by the Deliberating Council of Mar del Plata, was to allow the payment of municipal debts with products and services.[61]

◆ The Enemies of Social Currency

As the various cases demonstrate, social currencies face several challenges when implemented.

In principle, they suffer from a contradiction or dilemma between the scale of their acceptance and their value. To recapitulate, social currency has no intrinsic value (a prior use value) like commodity money, nor does it have a coercive authority to sustain it like legal tender. Its value derives directly from the trust of each community member, which is why such a dilemma arises. If the community grows too large, the relationships among its members become impersonalized and the general confidence decreases, affecting the currency (RGT case). If a strong currency is to be maintained, access to the community must be limited and ties between participating members must be strengthened (Poriahjú case). Similarly,

[59] Ibid., 84–86.
[60] Ibid., 87–88.
[61] Ibid., 88.

the community's growth requires centralization and delegation of trust to an authority, as well as hierarchization, whereas a small-scale community can maintain a decentralized and participatory organization.

In relation to this, as the scale increases and cohesion among participants decreases, malicious behavior becomes more likely, and the trustworthiness of the currency itself is compromised, as in the case of counterfeit bills.

> There were many people who were trained to be coordinators (...) But this did not guarantee that they would be good prosumers. If you are a jerk, you will remain a jerk all your life if you are a jerk. And what happened to us, that when a coordinator got upset, he would take everything: the credits, the list, even the boards, and to top it off, he would burn down the place - a place that was not ours because we operated in the clubs and schools. You could not control it.[62]

Coercion and competition are other problems that many of these initiatives faced. Tensions are generated between different initiatives, one against the other…

> …we traded with the credit of our zones (even today there are still fairs) and we were invaded by a network from Buenos Aires, the RGT, which organized parallel fairs to destroy our criteria of local organization;[63]

… as well as between the alternative economies, state authorities, and business community. In addition to the case of the RGT, explained in the chapter dedicated to that market, Poriajhú also had its share of incidents:

> We had death threats, harassment and things became difficult.
>
> (...) Because they give you the [welfare] plans, but in exchange for many silences, don't say anything, don't go there, don't do this, don't let them see you do such and such, forcing them to go on certain rallies, because it is the way to return the favor of the subsidy. (Interview with Marita, 11/18/2007, Capitán Bermúdez).[64]
>
> The monster was fed to grow. At one point we said that barter was being turned into a universal welfare public policy.[65]

[62] Ibid., 94.
[63] Ibid., 77.
[64] Orzi, Borrello, Costa, et al., *Moneda Social y Mercados Solidarios II: La Moneda Social Como Lazo Social*, 220.
[65] Orzi, Borrello and Plasencia, *Moneda Social y Mercados Solidarios I: Potencial Emancipador y Pedagógico de los Sistemas Monetarios Alternativos*, 95.

Although in some cases, such as Venado Tuerto, cooperation between government authorities and alternative markets has been achieved, when these markets threaten official authority or unofficial power networks, they are easily targeted by diverse types of external attacks, which add to the difficulties and internal conflicts that this type of initiative entails.

Theory II: New Paradigms

This is the second theoretical section. Having presented all the empirical material in the two previous sections, I will now introduce new paradigms proposed within economic science to approach the study of currency and money, aiming to overcome the limitations of the metallic paradigm addressed in the first theoretical section.

This section has only two authors, of whom I consider Mostafa Moini, the first, to be the most relevant.

◆ General Theory of Credit and Money

In 2001, the Review of Austrian Economics published a theoretical article in which the author, Mostafa Moini, an economist at the University of Oklahoma, proposed a new paradigm for the study of money. Not much was written about the life of this author. His obituary briefly recounts his academic career: born in Iran in 1939, he studied there until high school and pursued his higher education in the United States.[1] recounts his academic career briefly: born in Iran in 1939, he studied there until high school and did his higher education in the United States. He lived for a while teaching in a Master of Business Administration program at Harvard Business School in Iran, but the 1979 revolution closed it down. He continued to live there as an entrepreneur until 1987, when he returned to the U.S. He served as a lecturer at the University of Oklahoma until his passing in 2010.

The main argument made by this author is as follows:

> Money has always been and will always be one and the same thing, namely, a certain species of Right. Monetary instruments, on the other hand, have assumed a bewildering variety of forms at different times and in different places, ranging from animal skin and beads to strings of electronic pulses.[2]

Starting from that premise, he allows us to think at a higher level of abstraction than any of the theories previously explored in this paper. He is simultaneously coherent with the ethnographic evidence presented. In Moini's opinion, at least three authors came close to developing the concept of money in a way that aligns with his understanding. These authors are the ones I reviewed in the section "Money and Credit" of this paper: Walras, Wicksell, and Macleod. He says of the first one:

> But, in so far as monetary theory is concerned, Walras provided no additional contributions beyond those already mentioned. Having obtained such important analytical results, he began at this point to depart from his customary mode of investigation in which he would proceed faithfully in the spirit of pure theory to extract all the significant implications of what had been established already. Instead (…) he succumbed to empiricism.

[1] "Mostafa Moini Obituary," The Oklahoman (2010).
[2] Moini, "Toward a General Theory of Credit and Money," 270.

> Were it not for this unfortunate event, he would have been forced (by the logic of what he had already discovered) to formulate a theoretical payment system, one in which no medium of exchange would be required but only an etalon and a banking system. The payment system would then operate effectively as banks would credit and debit the accounts of the members of the payment community in line with the rights and obligations that arise as a result of their ongoing transactions.[3]
>
> In sum Walras ended up re-entangling the very things which he had worked so hard to disentangle, namely, the two concepts of unit of account and medium of exchange. This was undoubtedly a backward step in the development of monetary economics. Now more than a century later the said entanglement continues to act as the principal stumbling block in the path of development of monetary theory.[4]

To his surprise, the system he spoke of was not proposed by any economist other than Wicksell. Regarding his "pure credit system", Moini notes that he also came remarkably close to revealing the relational character of money, but that the constraints of the metallic paradigm prevented him from reaching such conclusions:

> Although he used such a system with great advantage in his analysis, Wicksell failed to notice its relevance to the investigation of the nature and origin of money. He remained entirely confined within the tangible medium-of-exchange paradigm, relying on metallic money and the "velocity of its circulation" as the primary concepts of his monetary theory.[5]

Of course, Macleod is the third to be on the verge of breaking the notion of the money thing, as I explained in the chapter dedicated to him. However, this economist did not enjoy as much importance as the other two.

> To this day economists consider money as a primary and credit as a derived notion. They define credit in terms of money, and consider the practice to be too obviously true to need any justification! But this only manifests the extent of the hegemony of the prevailing paradigm. The relation between money and credit, far from

[3] Ibid., 277–78.
[4] Ibid., 279.
[5] Ibid., 280.

> an obvious triviality, constitutes the very core of the problem of understanding the nature of payment systems.[6]

The development of electronic means of payment and the Internet highlights the problem of monetary theory, specifically the issue of money as a physical entity, making money appear more commonly immaterial.

> If positive balances on smart cards function like currency, why shouldn't they be called money, instead of credit? Perhaps, in the world of cyber-finance, everything should be called credit, demand deposits included! That is certainly the sense in which Wicksell used the term credit in his "imaginary pure credit system" (…). Clearly some fundamental rethinking of the terms, money and credit, is in order.[7]

In this rethinking, "a fundamental distinction must be drawn between money and monetary instruments,"[8] because:

> In the absence of the said distinction between money and monetary instrument these two radically different meanings remain fused together and are latently present in every application of the term "money."[9]
>
> While the said equivocation has acted as the principal retarding factor in the development of monetary theory throughout its history, in the era of Information Technology it proves even more paralyzing. In this sense the technology-driven evolution of the payment system is in itself forcing the economists to investigate the possibility of important substantive relations between money and information.[10]
>
> In the form of electronic checkable deposit, the instrument representing money exists as an information entity only, lacking mass, volume, shape or any other corporeal feature (as far as practical human interest is concerned, the physics of the problem being irrelevant). Such absence of any reference to sensible qualities challenges the habitual image that money must be something physical, and points toward the notion that the essential function of a monetary instrument resides in its ability to serve as a device for recording and conveying information about monetary rights.[11]

[6] Ibid., 281.
[7] Ibid., 270.
[8] Ibid.
[9] Ibid., 271.
[10] Ibid.
[11] Ibid., 270.

> This insight exposes the emptiness of the notion of money as "anything that serves as a medium of exchange." (…) the notion must be abandoned in favor of the theoretically promising concept of money as *unconditionally transferable credit.*[12]

This is synthetically the theoretical basis of the new paradigm proposed by Moini. As an Austrian school economist, he does not think that the development of money as a phenomenon will occur thanks to theoretical advances, but rather the other way around. He considers that money will continue to develop, and that theory must be up to understanding it. He already sees the end of physical monetary instruments coming. That money will be presented only as something immaterial:

> Money will come to assume, exclusively, the form of a pure accounting entity—an abstract category—, which varies as a particular account is credited at the expense of debiting one or more other accounts.[13]

But the problem is not only to consider money as a material versus an immaterial thing, but to consider it as "as a *thing*, that is, *an entity that can stand by itself*, rather than as a relation involving at least two persons."[14] Here we find again the Marxist problem of fetishism. Although Moini does not express it in those terms, since he belongs to another school of economics, he explicitly refers to this phenomenon of a relation between persons being understood as a relation between things or, more precisely, as a thing. What, not Marx but later Marxists, called reification.[15] It is a curious fact that neither Marx nor later Marxists have realized this characteristic of money and made the mistake of reifying it themselves.

Facing the erroneous conception of money as anything that serves as a medium of exchange, Moini proposes to think of money as "*a definite form of social relation in the sense that its very conception involves a right-obligation coupling between persons within the payment community.*"[16] He proposes that the new general theory of money and credit is built upon

[12]Ibid., 271.
[13]Ibid.
[14]Ibid., 272.
[15]Georg Lukács, "Reification and the Consciousness of the Proletariat, I. The Phenomenon of Reification" In *History and Class Consciousness: Studies in Marxist Dialectics*, (The Merlin Press Ltd., 1971).
[16]Moini, "Toward a General Theory of Credit and Money," 272.

"the basis of Macleod's credit view of money and Walras's *numeraire* and *etalon.*"[17]

> ...any payment system has only two fundamental requirements: (1) an *etalon*, and (2) an information system that records—in terms of the *etalon*—the rights and obligations that arise in the course of transactions between the members of a payment community.[18]

Another fundamental concept in his theory is money's dual nature: "It means one thing from the perspective of the individual, and another thing from that of the payment system as a whole."[19]

> Each of the two perspectives has led to the development of a distinct set of monetary concepts that have evolved in separate channels. This dichotomy is perhaps one of the chief factors responsible for lack of progress in understanding the nature and origin of money. Reconciliation of the two aspects is a sine qua non of further progress in monetary theory. This is attained by the credit-view of money.[20]
>
> As a reckoning factor, money is not subject to a person's preference structure. It is rather an externally given fact confronting the person as a nexus of information (...). Thus from the system-theoretic perspective money is not a thing but a relation, or rather a system of social relations. On the other hand, from the personal perspective, money is a good, a thing that supplies the individual with utility, and it is, therefore, subject to the preference structure of the person who holds it.[21]
>
> Credit is a relationship of trust and confidence between two or more persons. (...) For this reason it may be asserted that credit is necessarily a social relation as opposed to a thing. What differentiates credit from other social relations is the fact that *it arises from the exchange of goods and services* between two or more (natural or legal) persons. *Should it be possible to establish that money, in whatever form, is a species of credit, then money too will have to be viewed as being a social relation rather than a thing.* The idea that money is a species of credit may appear to contradict the "obvious" truth that credit instruments consist of claims to money. If credit is a claim to money, then money must be prior to credit, both in concept, and

[17] Ibid., 273.
[18] Ibid.
[19] Ibid., 274.
[20] Ibid.
[21] Ibid., 275.

> in daily practice, now and throughout history. Such is indeed the appearance of the mater [sic].[22]

As Mauss stated and as can be seen exemplified in many of the cases surveyed in the empirical section, this was never the case, and it could even be said that credit often precedes the medium of exchange. What Mauss explained about the gifts that are given and returned, Moini translated into proper economic terms:

> Credit is the present right to a future payment (Macleod 1893:88). The form or substance in which the payment is to be made is in every case specified or understood in the course of the transaction that gives rise to the credit.[23]

There does not have to be money for credit to exist, only exchange and loans. What is given by whom to whom, and what is returned to whom, are circumstantial.

> Credit stands prior to money, both logically and historically. *Money is a species of credit, and its development can be understood only as an aspect of the general process of evolution of credit.*[24]

After establishing this principle, he explains the logical and historical succession, including how to move from indirect valuation to the unit of account.

> Einzig, in his unique and impressive survey of ethnographical studies of money, correctly observes that the conception of Hildebrand according to which there were "three stages of evolution, natural economy, money economy, and credit economy, is entirely wrong...
>
> Loans of nonspecific (fungible) things such as grain, as opposed to identifiable (nonfungible) ones, like animals or tools, may have served as basis for the development of, not only the standardized commodity, but also measurement units of all kinds.13 It is evident that such units had to have developed prior to the development of a unit of account (Homer 1963:19). And the latter tends to develop as instances of inconsistency between direct and indirect valuation of goods and services are noticed and gradually narrowed.
>
> Thus the process of development of consistency of exchange ratios between various goods and services did not have to wait until the emergence of well-developed markets, as is widely believed. It started

[22] Ibid., 281.
[23] Ibid., 282–83.
[24] Ibid., 283.

already at the dawn of history, as primitive man attempted to evaluate things that he had to give or receive in the context of the web of mutual rights and obligations that characterized the extended family and tribal modes of existence. In this process indirect valuation would be unavoidable.

Indirect valuation is not the same thing as indirect exchange. The former constitutes a presupposition for the latter and, as such, comes prior to it both in logic and in history.[25]

Because in primitive societies valuation was applied to everything, indirect valuation must be viewed as being as old as history: Things obtained as gift, or through war, theft and loan would all be subject to valuation, even if in quite crude terms (Homer 1963:18). So would objects of prestige, of use for personal ornament, or of interest for decorative purposes, such as human and animal skulls. Some of these often developed into a kind of currency (Einzig 1948:378). Malinowski and others showed that the same considerations apply to objects of religious or ceremonial significance (Einzig 1948:379).

(…) *The possibility, or rather the indispensability, of emergence of indirect valuation in primitive societies means that a unit of account could have emerged in these communities quite irrespective of the presence or absence of some sort of medium of exchange.*

(…) In sum, a duty to pay arose in the course of loans in kind, and also as a result of a large number of social and religious factors. Ancient communities were held together by means of a rigid set of rights and duties, which were rooted in and enforced by custom. For many millennia the rights and obligations that arose out of voluntary exchange were, at best, minimal and only on the periphery of the daily life experiences of the individual. Menger and other economists have failed to notice the role of customs and coercion (by the state or religious institutions) in the development of units of account. They have failed to note that voluntary exchange is only one among many circumstances that may lead to the emergence of a duty to pay.[26]

A duty to pay is one side of a relationship of which a right to receive constitutes the other. The relationship itself may be referred to as either a credit or a debt relationship. That in primitive communities such relationship arose primarily out of religion and custom, as opposed to formal exchange, should in no way detract from their essential content as forms of credit relations. Thus credit is as old as

[25] Ibid.
[26] Ibid., 284.

> history, and resides at the very core of the social mode of existence of man.
>
> The above findings lead to the following conclusion: Units of account evolved in ancient communities not in connection with barter and market exchange, but on the basis of credit relations, which arose in relation to loans in kind, gifts, religious duties, offerings, ransom and many other factors.[27]

Then, the unit of account becomes the medium of exchange:

> …the prevailing view that units of accounts developed as byproducts of market exchange, and on the basis of the exigencies of indirect exchange, is without logical and historical foundation. Even in modern times the two aspects have at times stood separately and independently from one another. On numerous occasions in recent history—whenever the medium of exchange in use in a particular community has ceased to have a stable value—the unit-of-account and medium-of-exchange have separated into independent functions.[28]

This means, for example, that if there is significant currency instability in Argentina, certain products, which are generally imported, are valued in dollars, although they are paid for in pesos. Thus, the medium of exchange is the peso, but the unit of account is the dollar. He also quotes Einzig in reference to abstract units of account, such as the case of the Akumal, which I mentioned in the chapter dedicated to that author.

> Based on the above findings it may be concluded that while the unit-of-account aspect of money is essential and indispensable, the medium-of-exchange aspect is incidental and dispensable.
>
> (...) Thus, far from being historical curiosities, the "fictitious monetary units" just noted point toward the very essence of money, money stripped from all its historical and contingent aspects. The significance of the findings presented so far in this paper cannot be overstated: *Whereas Walras established (and Keynes fully grasped) the logical priority of the unit of account over the medium-of-exchange concept, anthropologists and historians showed its historical priority. In other words, both in logic and in history, the concept and fact of unit of account is prior to and independent from those of medium of exchange.*[29]

[27] Ibid., 285.
[28] Ibid.
[29] Ibid., 286.

> He then separates three concepts that are confused in economic theory: money, medium of exchange and monetary instrument:
>
> *…a medium of exchange—gold or whatever else—is not money, and money is not a medium of exchange. Money is an abstract right, credit; and any medium of exchange is some specific means (from among many possible ones) for representing that right.* It functions merely as a recording instrument, as an evidence that a person has either delivered or has promised to deliver a certain value of goods and services to others. Being a token or representation of money, any medium of exchange—be it shells, beaver skin, gold, paper currency, or demand deposits (electronic or paper-based)—should be viewed as a type of *monetary instrument, not money*, as is usual case. This distinction happens to be of enormous theoretical significance.[30]

He draws on cases of payment systems built on human memory to add weight to his argument. Just as Boas observed, as quoted by Mauss, cited here, that societies without writing make transactions in public to leave a record, Moini observes that:

> The monetary instrument initially at work in primitive communities consisted of standing balances of "accounts" recorded and maintained by reliance on human memory. The memory functions went on both at the (intra-cerebral) level of individuals, and at the (inter-cerebral) level of the community with its (historically-accumulated) stock of cultural mores and mechanisms against lapses of memory or fraud.[31]

And even though there are multiple forms, written, oral, material, or abstract, of keeping this record:

> What is common between these radically different forms of monetary instruments is that they all serve the same two principal ends. (a) *As evidence of possession* of the right to have access to a definite value of the community's stream of goods; and (b) as an *instrument for transferring* such right to another person.[32]

Moini credits anthropologists for making this finding when they encountered the inapplicability of the concept of money, inherited from

[30] Ibid., 287.
[31] Ibid., 290.
[32] Ibid.

nineteenth- and twentieth-century economists, in their field studies. However, he also notes that they have not developed a superseding concept or theory based on it. That is the task that he set out to accomplish.

> The digital payment system and the primitive one that relied on human memory have this in common that they both rely on an information system explicitly, in contrast with the variety of payment systems that came between the two, which do so implicitly. Thus money seems to have completed a full round of the evolutionary spiral. If the story of man is "from dust to dust", that of money is "from information to information."[33]

But he warns, again, that it is not enough to consider it as information, as an immaterial thing, since in this way it remains a thing (reified). It is necessary to consider it as a relation, a right.

As the next step in establishing the new theory, it seems necessary to unify the theories of utility and money. The field of study of money is separated from that of value and distribution. "Such lack of progress," he points out, "appears to be rooted in two factors: (1) reliance on a faulty concept of money; and (2) reduction of the subjective theory of value to a mere aspect of itself, namely, the marginal-utility concept."[34] He then explains what has been lost from the subjective theory of value that could allow further progress in studying money.

> Being a subjective affair, *utility is not an abstract category, but one that is person-specific, and event-specific.*
>
> (...) Because a person lives in time and space and directs her diverse interests toward a differentiated world, utility is not a simple, but a multidimensional variable. (...) for any given person, utility of a good or service depends on its quality, quantity, location, timing, and the degree of assurance associated with it. I shall refer to these as the Fundamental Dimensions of Utility (FDU).
>
> (...) It should be noted that whereas FDU applies only to consumers, similar considerations are true of producers. (...)In this case we may speak of the dimensions of (customer) *value* rather than *utility*. It is therefore necessary to coin a more general term than FDU, namely, the Fundamental Dimensions of Value (FDV). This is not a substitute for but a more general category than the former, in that

[33] Ibid., 292.
[34] Ibid., 296.

value would mean utility in case the evaluating person is a consumer, and profitability, in case the evaluator is an entrepreneur.

(...) These dimensions have been coped with in separate analysis: in capital theory, location theory, and theories of risk and insurance. However, as fruitful and unavoidable as the adoption of this strategy may have been, it should be recognized that it has led to a fragmentation of economic theory. Essential as analysis with respect to each of the dimensions is, a fuller understanding of the actual economic phenomena requires a synthesis of the separate results. However, quantitative analysis is unlikely to succeed in this respect, because the multidimensional analysis required for the purpose would be too complex, given the present state of the science. Qualitative analysis based on the proposed concept of FDV may prove to be the only alternative for the purpose, as it supplies a comprehensive framework within which the category of value may be grasped in its entirety.33 The resulting comprehensive view of the problem can serve two primary purposes: (1) It can help in bridging the gap between economic theory and the actual working of the economy; and (2) it can open new avenues of research into the nature of the relation between money and prices.

The connection between the theory of value (as stated above) and money is straightforward. Among other things, money relieves a person (or a firm) from the burdens and costs of having to carry large inventories of consumer or producer goods, as the case may be. If money is an abstract right of access to all that is customarily available in an economy, then a person can choose to hold limited, convenient amounts of various goods, relying for the rest on the inventories of specialized traders from which she may replenish her stocks periodically as desired. (...) Enormous economies are realized by relying on the market, instead of carrying the required inventories individually. Because, directly or indirectly, all production is production of utility along one or more of the FDV, the laws of large-scale production are applicable as much to production in the service sectors, retailing or otherwise, as to farming, mining, or manufacturing. *The difference lies only in the fact that each line of production enhances utility (or profitability) along a different mix of the FDV*

(...) Among other considerations, money enables the individual (consumer or entrepreneur) avoid the necessity of carrying large stocks of goods for future consumption or use. This individually moti-

> vated factor then serves as the basis for the realization of the kind of money-driven scale economies discussed above.
>
> (...) Because among other things, money provides its holder with this service, it must be treated as a good, one that supplies its holder with choice-value. Being a good, money necessarily falls under the domain of utility theory in general and the law of diminishing marginal utility in particular. This result is of enormous analytical interest as it amounts to a *unification of the hitherto separate and unconnected theories of money utility.* Two critical theoretical constructs have made this integration possible. (1) The theory of abstract rights and its connection to money, due to Macleod; and (2) the concept of Fundamental Dimensions of Value, which has existed hitherto *implicitly* in the works of all economists, but has been given a formal and explicit treatment in this paper.
>
> (...)An interesting by-product of the foregoing analysis is worth noting. It is now possible to provide the important notion of liquidity with an economic content and to embed it securely within the framework of utility theory: *Liquidity of an asset resides in the choice-value supplied by it to its holder.* Because a monetary claim is free from all conditionality, it supplies its holder with the highest degree of liquidity. (...) In this way liquidity assumes the status of a well-defined theoretical concept within the framework of the General Theory of Credit and Money.[35]

After these definitions, he goes on to define money, also unifying the various theories about it:

> ...money may be defined, from the perspective of an individual, *as a right that provides its holder with choice-value.* This right is recorded by means of some sort of monetary instrument.[36]
>
> *Money is a general claim* against the stream of customary goods and services of a community, whatever the goods and whoever the person in possession of the goods. In other words money is a type of right that provides its holder with unconditional choice, and therefore, with the highest degree of choice-value.[37]

And from another angle, concerning credit:

> *Because anything that is potentially available for sale necessarily belongs to someone somewhere within the payment community, un-*

[35] Ibid., 296–99.
[36] Ibid., 299.
[37] Ibid., 300.

> *conditional transferability of credit constitutes the necessary and sufficient conditions for the emergence of abstract credit.* By definition a transferable credit is a right which may be exercised at any time, anywhere, against anything or anyone who offers things for sale. Transferable credit is socialized credit. (...) *Money is unconditionally transferable credit.*[38]

These two definitions correspond to the dual aspect of money I mentioned earlier: the aspect from the individual's point of view and the comprehensive view of the payment system. Moini explains that these definitions are not, as hitherto considered, mutually exclusive or incompatible. On the contrary, it is because money is an unconditionally transferable claim that it provides the individual with unconditional choice value.

He then explains the components of a payment system: the unit of account and the medium of recording. He emphasizes that economics is not concerned with studying the various tools that perform the function of recording transactions, i.e., monetary instruments, since these are cultural, legal, or technical matters, not economic ones. And, by analogy, if money is the most abstract species of credit, "A monetary instrument is not just any credit instrument, but the most abstract species of such instruments."[39]

◆ Quantum Theory of Money

In 2018, David Orrell, a PhD mathematician from Oxford University, published a book on this topic, titled *Quantum Economics: The New Science of Money.*[40] This new theory is presented as a compelling analogy between physics and economics, aiming to shift the neoclassical-mechanical paradigm to a quantum paradigm. In his introduction, he says:

> Money is a way of combining the properties of a number with the properties of an owned thing. The fact that numbers and things are as different as waves and particles in quantum mechanics is what gives money its unique properties.[41]
>
> …the information encoded in money is a kind of quantum entanglement device, because its creation always has two sides, debt and

[38] Ibid., 301.
[39] Ibid., 304.
[40] David Orrell, *Quantum Economics: The New Science of Money*, (Icon Books, 2018).
[41] Ibid., 15.

> credit. And its use also entangles people with each other and with the system as a whole…[42]

It is similar to Moini's theory in form, but Orrell uses quantum physics terminology in its development. I do not intend to elaborate too much on this theory, but I did not want to overlook it either; therefore, I will limit myself to transcribing and presenting his restatement of certain economic concepts:[43]

> **Money**. During the gold standard, money was thought to be a real thing, while today it is more commonly seen as a number representing virtual government-backed debt, except for cyber currencies which don't quite fit with either picture. We will show that money is both real and virtual, in the same way that light is both particle and wave.
>
> **Value**. Classical economists such as Adam Smith believed that money was measuring labour, neoclassical economists that it measures utility. According to quantum economics, money is measuring – money, which is a form of information.
>
> **Pricing**. In conventional theory, prices are thought to be determined by imaginary supply and demand curves, which – as we'll see – have no empirical backing. Quantum economics shows that price is an uncertain property which is in a sense created through transactions – just as a particle's position or momentum is inherently indeterminate until measured. This has implications for areas such as quantitative finance, but also for the dynamics of things like the price of your house or the value of your pension.
>
> **Debt**. Mainstream economics treats debt as something that comes out in the wash – what one person owes, another is owed, so they cancel out. According to quantum economics, though, debt is a force that entangles people, institutions, and the financial system as a whole in ways that are difficult to understand and potentially destructive. This is a concern, given that global debt is now estimated at over $200 trillion.
>
> **Risk**. Mainstream theory assumes that markets are stable, efficient, and self-correcting. Quantum economics shows that none of these assumptions stand up, which means that the risk models currently taught in universities and business schools, and relied upon by businesses and financial institutions, are not fit for purpose (as many

[42] Ibid., 16.

[43] In the original, it was "translating," as this book was only available in English.

guessed after the last crisis). We need to update our approach to handling risk.

Decision-making. Mainstream models assume that consumers make rational decisions, with the occasional adjustment to account for behavioural factors such as 'bounded rationality' (i.e., the fact that we make decisions under informational and cognitive limitations). Quantum economics admits no such bound, and treats things like emotion and entanglement as integral to the decision-making process.

Finance. Mainstream models downplay or ignore the role of the financial sector, which is one reason financial crises always come as a surprise. Quantum economics puts money in its rightful place at the centre of economics, and offers new tools for understanding the financial system. Only by acknowledging the dynamic and unstable nature of the system can we find ways to better control it. Nowhere is this more true than with the quadrillion dollars'- worth of complex derivatives which hang over the economy.

Inequality. Mainstream economics was inspired by classical thermodynamics and concentrates on optimising average wealth (like the average temperature) instead of its distribution. But the dynamics of money tend towards disequilibrium and asymmetry. This helps to explain why a group of people who could fit into the first-class cabin of a jet now control as much wealth as half the world's population.

Happiness. Mainstream economics assumes that people act to optimise their own utility, which leads to maximum societal happiness. Quantum economics draws on the field of quantum game theory to show that the truth is more complicated, in part because people are entangled – and asks whether economics is the best tool for thinking about happiness in the first place.

Environment. As quantum cognition shows, context is important when we take decisions. The inbuilt biases of neoclassical economics have meant that for too long, we have been ignoring the wider environmental context, with very visible effects. Quantum economics points the way to an economics which can, not account for, but make space for fuzzy, uncertain quantities such as the health of ecosystems; while also addressing one of the main contributors to environmental damage, which is our money system.

Ethics. Just as money has been excluded from mainstream economics, so has ethics. One reason is that, as with classical physics,

> the economy has been treated as an essentially mechanistic system where things like will, volition, and personal responsibility seem to have no role. Another is the fact that, ironically, economics itself has been influenced by money. Quantum economics is the ethical alternative.
>
> **Modelling**. Orthodox models of the economy used by everyone from economists to central banks to policy-makers are based on a Newtonian, mechanistic view of human interactions and emphasise qualities such as stability, rationality, and efficiency. Quantum economics starts from a different set of assumptions, and leads to models that exploit techniques developed for the study of complex, living systems. A word of warning: this area is new, so while I will concentrate on tested methods, not all of the ideas and techniques described here have been demonstrated yet in an economics context. I will make it clear when that is the case.[44]

Between these two proposals for a new paradigm for monetary theory, I find the first one more appealing. Moini contradicts Mises's major postulate: that the primary (if not the sole) function of money is to serve as a medium of exchange. Mises was emphatic about how his Schools's modern theory of subjective value was superior to the classical labor-value theory, but he failed to overcome the metallic paradigm. Mises faced a logical problem: the utility value of money depends on its exchange value, and at the same time, the exchange value of commodities (including the commodity that serves as a medium of exchange) depends on their use values. Faced with this circular reasoning, the solution he devises resorts to a temporal dimension: a commodity only becomes a medium of exchange if it has been just another commodity, with some use value. Only in a second instance can it become a means of exchange, thanks to that first foundation of value. Fiat money and credit money, both lacking intrinsic value and use -value, are derivatives of commodity money and do not present problems according to this explanation.

However, this contrivance does not solve the logical problem posed. It depends on certain assumptions of economic theories: that pre-historic societies, without writing, without a State, etc., had immediate exchange relations, barter, and a form of currency or money to facilitate this exchange. As Mauss, Einzig, and Moini explain, the evidence does not sup-

[44] Orrell, *Quantum Economics: The New Science of Money*, 23–25.

port this assumption. Moreover, phenomena such as social currencies and cryptocurrencies are complex to explain in terms of Mises's theory.

Moini then presents a complete theory of money based on the subjective theory of value, starting from credit as the foundation of money and understanding money as a relation rather than a thing. Mises's taxonomy is still particularly useful, but no longer as a classification of types of money but of monetary instruments.

Having reviewed all these different theories of money and currency, I can conclude the first part of this work and apply them to the study of cryptocurrencies in the following chapters.

Part 2

Money and Cryptography

Bitcoin

Bitcoin, the subject of this thesis and which I have barely mentioned so far, is of enormous theoretical importance. In the first part, I elaborated extensively on currencies in general to gain a deeper understanding myself and, in turn, to provide the reader with an understanding of the state of monetary theory and the significance of Bitcoin within it.

Considering all the above, I can begin this study with the seemingly most straightforward question: how to place Bitcoin in the monetary taxonomy outlined above.[1] It has been argued that "Bitcoin is a commodity-money"[2] because it has an intrinsic value linked to its production cost, but I consider this to be disputable. The main problem with considering Bitcoin a commodity-currency is that it is not a commodity beyond being a currency. By this I mean that it has no prior use value; its only use is as an exchange value. The other categories are not more appropriate. Therefore, one must take a step back and ask whether Bitcoin is, in fact, a currency at all, and how monetary theories can explain this.

One of the first reactions that people have when they are introduced to Bitcoin for the first time is precisely to question its monetary status: "How can a number on a computer be money?", " What is it backed by?" and, even when they have already conceived of its existence and use: "How can it be exchanged for *real* money?" We could say that this skepticism towards Bitcoin separates the *nocoiner* from the *bitcoiner*,[3] the latter of whom has turned the terms of their questioning around by pointing it towards legal tender. "And why does the dollar (or any other national currency) have

[1] Although the authors mentioned in the first theoretical section speak of currency and money indistinctly, in keeping with the theoretical framework presented by Moini, I will mainly speak of currency, understood as a monetary instrument.

[2] Noel Jones, "Bitcoin is a Commodity Money," Bitcoin Theory, (2014).

[3] In the jargon of the Bitcoin community, *bitcoiner* refers to those who use and are in favor of Bitcoin; *nocoiner* refers to Bitcoin's detractors.

value?" is a question that baffles common sense. In Gadamer's words: "A question places what is questioned in a particular perspective. When a question arises, it breaks open the being of the object, as it were."[4] On a philosophical and ideological level, this is the effect that Bitcoin produced as an invention: the questioning of the legitimacy of legal tender and its issuer. This is no coincidence and responds directly to the ideological positioning of its first promoters, the people who called themselves cypherpunks or crypto-anarchists. Theoretically, this questioning is a phenomenon that tests the current paradigm or paradigms. The two are not independent of each other. Moini was aware that the paradigm he was proposing could have repercussions in the political sphere or, in other words, that the current paradigms serve to conceal specific mechanisms of power. I quote:

> In the context of the electronic model of the payment system noted there is no room for misunderstanding the nature of money, because there is no *thing* to be held and handed over to someone else as a means of payment. There are only accounts inside the (imagined) digital social balance sheet. Any change in one account must have its exact balancing changes in one or more other accounts. *All that occurs is transfer of rights.* The reality of money as a species of rights practically forces itself into the mind of the economist. All the mysteries that have surrounded money throughout its long history disappear for good. (...)The iron necessity of the laws of double-entry accounting will force the economist to recognize that her concept of money and credit must be meaningful not only from the perspective of individual holders of money but from that of the whole economy (...). [Such system-theoretic perspective leaves no room for arbitrary manipulations of the monetary rights of the people by the banks, the state, and the international agencies.] **The** commercial banks, the central banks, IMF, and the World Bank will have to defend themselves against the suspicion that their engagements in arbitrary forging of credit around the world may be acting as the primary causes of instability in the world economy.[5]

I understand that there are two prevailing paradigms. On the one hand, metallism remains prevalent in common sense and much of economic scholarship, which Moini refers to as thing-mindedness. On the other hand,

[4]Hans-Georg Gadamer, "Elements of a Theory of Hermeneutic Experience" In *Truth and Method*, Bloomsbury Revelations, (Bloomsbury Academic, 2013).

[5]Moini, "Toward a General Theory of Credit and Money," 293–94.

its alternative is the statist paradigm, derived from Knapp's notions that the government creates money. This encompasses a broad spectrum of theories, including chartalism, Keynesianism, and monetarism. I did not review these theories beyond Knapp's because they are not concerned with studying money scientifically as a phenomenon, but rather with proposing the best decision for a government to make regarding its domestic economy, utilizing its authority to issue money. Arguably, their object of study is not money but monetary policy.

Figure 11. Bitcoin isotype used by core developers and in Bitcoin Core client.

Bitcoin cannot be explained within any of these paradigms. In principle, I rule out the statist paradigm for obvious reasons: Bitcoin is not "a creature of law", as Knapp defined currency, yet it is a monetary instrument. The difficulty with the "thing-money" or "medium of exchange" paradigm is not immediately apparent. Bitcoin is not just a digital currency, nor does it represent the invention of digital currency. Wicksell had already spoken of virtual money when referring to credit notes in circulation; digital or virtual means of payment had already existed for at least a decade when Bitcoin was invented. The fundamental difference is that Bitcoin does not represent deposits, credits, or balances in 'something else', like all previous systems. Bitcoin is that "Ideal bank" of "pure credit" that Wicksell envisaged, but without a bank and immobile reserves in vaults. Bitcoin is not a 'thing', and not only because it is information, but also because it is nothing more than an extensive database with debits and credits of amounts that represent nothing outside that very system. That is, it does not work in reference to any value external to the system itself.

Nor are cryptocurrencies social in the sense of interpersonal, since they do not require trust in the entities that issue them, the other party to a transaction, or intermediaries. It is the protocols and mathematical laws by which they operate that are trusted. It is a balance between anonymity (or pseudonymity) and transparency. All transactions are transparent and public, so anyone can view them, but they do not disclose personal in-

formation about those carrying them out. Also, the decentralized nature of its functioning is ensured by rewarding cooperating actors, so that acting against each other becomes detrimental behavior for the actor himself. They cannot be "cheated" because the rules of the game are embedded in its functioning. A judge or coercive authority does not administer rewards and punishments, but rather by the software it runs on. Moreover, the rewards or punishments only have scope within the system; there is no extra-economic coercion. This gives them a non-hierarchical and deterritorialized character, but more importantly, it means that laws are no longer something to be enforced from the outside; they are endogenous to this monetary instrument. And so, they are a new money paradigm that can be extended to other social institutions.

This leads an author like Mark Alizart to think of an oxymoron or paradox, and that in reality, the widespread use of blockchain technology leads to a different social system than Bitcoin enthusiasts intended. He says:

> [Bitcoin] seeks to restore institutions we can believe in, not burn them to the ground. It wants to make this society liveable. And in a very compelling sense, it does so in the same way as the Reformation and the revolutions did: by replacing old institutions with new ones, which are more robust only because they are *chosen* institutions. **Bitcoin frees us by allowing us to impose chains upon ourselves**, as the appropriately named *blockchain* clearly indicates. (…) The theological-political regime of crypto will not be 'cryptoanarchism'; quite the contrary, it will be a regime that will impose a new law on us, a new common law, more austere than liberal laws, thus more like a regime that too deemed itself to be revolutionary in its time, even if it didn't succeed in bringing about the revolution its believers had hoped for: namely, communism – or, more precisely, *cryptocommunism*.[6]

Throughout this second part, I will explain the technical aspects that enable Bitcoin to function in this manner and examine its qualities as a monetary phenomenon. To do so, I will use Einzig's scheme,[7] which was inspired by Jevons's work.[8] I will also use theoretical tools from the

[6] Mark Alizart, Cryptocommunism (Theory Redux, 2020)

[7] Einzig, P*rimitive Money in its Ethnological, Historical and Economic Aspects*, 308–530.

[8] Jevons, *Money and the Mechanism of Exchange*.

different schools of thought I reviewed in the first part. A fundamental distinction that Einzig makes, but I will ignore, is between primitive and modern money. I will refer only to monetary instruments in the broadest sense, as defined by Moini, encompassing all their manifestations, from the most unusual cases reviewed in the first part to cryptocurrencies. The only comment I will make in this respect is that, despite being a more advanced technology than what the author calls "modern money," cryptocurrencies, due to their dynamics, are more like what he defines throughout the volume as "primitive money." For example, let us recall Mauss's assertion that societies without writing (and I add, without authorities) made transactions public to ensure their legitimacy. There would certainly seem to be an evolutionary circle "from information to information, [passing through the material]."[9] and 'from consensus to consensus, passing through authority.'

[9]Moini, "Toward a General Theory of Credit and Money," 292.

◆ Origin

As Mauss said in 1914, there is no point in trying to find THE origin of currency or money, a single or universal origin in which all money was invented once and for all. Still, we can see how different processes can lead to the same result. The previously discussed ethnographies and social currency experiments leave straightforward evidence that monetary instruments are created, destroyed, and transformed in various ways according to circumstances. Among these possibilities, what I can do is to see which best explains the advent of cryptocurrencies as a medium of exchange or whether they are, in fact, a more abstract form of money that foregoes the medium of exchange.

First, I will name the theories or hypotheses that least fit the case of cryptocurrencies, quickly discard them, and continue with the ones that are of interest. These are: origin through ceremonial and ornamental use,[10] religious,[11] political,[12] matrimonial origin,[13] and origin through status symbol.[14] All these origins have in common a first non-mercantile use of a material good, which makes it acceptable to most of a community and suitable to become a means of exchange. However, Einzig recognizes that the opposite phenomenon can occur, that a good, by being a currency, becomes a means of payment of tribute, a symbol of social status, a religious/ceremonial sacrifice/payment, or a form of payment for wives. This is clearly not the case with cryptocurrencies, since they have no physical qualities that make them useful or attractive in a ceremonial or ornamental way.

Cryptocurrencies have the quality, shared with legal tender (fiat currency) and social currencies, of being created to serve as a monetary instrument; unlike commodity-currency or credit-currency. In this sense, all three have a first lack: a use value as a commodity. Cryptocurrencies and social currencies also have a second shortcoming: there is no authority sanctioning their use by a given community, as there is for legal tender. At the beginning of Bitcoin, cryptocurrencies were in a situation more like that of social currencies. However, as I showed in the section on them,

[10] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 377.
[11] Ibid., 380.
[12] Ibid., 387.
[13] Ibid., 393.
[14] Ibid., 396.

social currencies tend to arise in groups with a certain cohesion and trust among their members. Because of its very ideological nature and the environment in which it originated, Bitcoin has this third shortcoming. One of its characteristics is that it does not depend on interpersonal trust, which is why it is called trustless.

Bitcoin and cryptocurrencies are viable forms of something attempted at least two decades earlier. One of their first antecedents can be found in David Chaum, who proposed, already in the early 1980s, Blind Signatures for Untraceable Payments, which consisted of the following:

> A fundamentally new kind of cryptography is proposed here, which allows an automated payments system with the following properties:
>
> 1. Inability of third parties to determine payee, time or amount of payments made by an individual.
> 2. Ability of individuals to provide proof of payment, or to determine the identity of the payee under exceptional circumstances.
> 3. (3) Ability to stop use of payments media reported stolen.[15]

Specific ideas about the implications of such technological advances began to circulate in certain political circles:

> …the public-key cipher (with a personal computer to run it) represents an equivalent quantum leap—in a defensive weapon. Not only can such a technique be used to protect sensitive data in one's own possession, but it can also permit two strangers to exchange information over an insecure communications channel—a wiretapped phone line, for example, or skywriting, for that matter)—without ever having previously met to exchange cipher keys.[16]

The public-key or asymmetric cryptography referred to in that paragraph is one in which messages are encrypted with one key and decrypted with another. Unlike symmetric cryptography, in which the same key encrypts and decrypts messages. The decryption key is kept private, and the encryption key is public. This system has various applications:

[15] David Chaum, "Blind Signatures for Untraceable Payments," Advances in. Cryptolology, (1983) 199–203.

[16] Chuck Hammill, "From Crossbows To Cryptography: Techno-Thwarting The State," (1987): 3.

- Since the public key encrypts messages, and the private key decrypts them, only the recipient of the message can read it. This type of system is used, for example, in PGP, an encryption method for email, so that anyone can send messages to an address, but only its owner will be able to read them.

- The public key can validate messages signed with the private key. Only the sender of a message can make messages valid for that public key. This system is used to make digital signatures, as it is easy to prove that a message was written by the holder of that private key. It is this signature mechanism that will be used by cryptocurrencies to verify their transactions.

During the 1980s and 1990s, this led to the formation of virtual communities dedicated to developing cipher tools as a form of anarchist militancy. In their documents, it is made clear that the development of an autonomous form of money is one of their fundamental interests:

> These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.[17]
>
> We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.[18]
>
> We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.[19]
>
> The World Wide Web is growing at an explosive pace. Combined with cryptographically-protected communication and digital cash of some form (and there are several being tried), this should produce the long-awaited colonization of cyberspace.[20]

None of these early instances of digital cash were remarkably successful, so they did not gain widespread recognition beyond the communities that

[17] Timothy C. May, *The Crypto Anarchist Manifesto* (1992).
[18] Eric Hughes, A Cypherpunk's Manifesto (1993).
[19] John Perry Barlow, A Declaration of the Independence of Cyberspace (1996).
[20] Timothy C. May, Crypto Anarchy and Virtual Communities (1994).

attempted to implement them. However, many of them contained elements that were later used in Bitcoin.

> I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.
>
> Until now it's not clear, even theoretically, how such a community could operate. A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. (…)
>
> I will actually describe two protocols. The first one is impractical, because it makes heavy use of a synchronous and unjammable anonymous broadcast channel. However it will motivate the second, more practical protocol. In both cases I will assume the existence of an untraceable network, where senders and receivers are identified only by digital pseudonyms (i.e., public keys) and every message [sic] is signed by its sender and encrypted to its receiver.
>
> In the first protocol, every participant maintains a (separate) database of how much money belongs to each pseudonym. (…)
>
> In the second protocol, the accounts of who has how much money are kept by a subset of the participants (called servers from now on) instead of everyone.[21]

Wei Dai presented his idea, B-Money, in 1998. This system, as he explains, uses asymmetric cryptography to verify transactions. The sender signs them to give them validity, with a first key pair and a second cipher that only allows the recipient to see them. He thought of a system where each user could sign their private key to prove a transaction's validity, but he could not adequately solve how to keep a record of all those transactions.

In 1997, only a year earlier, Adam Back developed an algorithm called "hashcash":

> The hashcash CPU cost-function computes a token which can be used as a proof-of-work. Interactive and non-interactive variants of cost-functions can be constructed which can be used in situations

[21] Wei Dai, B-Money (1998).

> where the server can issue a challenge (connection-oriented interactive protocol), and where it can not (where the communication is store–and–forward, or packet oriented) respectively.[22]

This proof of work refers to a proof, in the sense of demonstration, that a quantity of computational work was performed. It consists of presenting, as it says, a challenge for which the solution is not known but is easy to prove once performed. The challenge involves performing a series of computations, not exact but estimated, so the solution functions as evidence or proof that a certain amount of work was performed. This system did not contain and was not intended to include elements of currency. However, it did present something more fundamental: some formal and practical application of the labor-value or production cost theory. I will expand more on this in a later chapter.

Nick Szabo proposed, also in 1998, another approach to a fully digital form of money, which he called bit gold:

> A long time ago I hit upon the idea of bit gold. The problem, in a nutshell, is that our money currently depends on trust in a third party for its value. (...) Thus, it would be very nice if there were a protocol whereby unforgeably costly bits could be created online with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust. Bit gold.
>
> My proposal for bit gold is based on computing a string of bits from a string of challenge bits, using functions called variously "client puzzle function," "proof-of-work function," or "secure benchmark function". The resulting string of bits is the proof of work. Where a one-way function is prohibitively difficult to compute backwards, a secure benchmark function ideally comes with a specific cost, measured in compute cycles, to compute backward.[23]

Szabo's approach was to apply Back's proof of work to assign an autonomous value (independent of a third party) to a digital object, specifically this bit string, hence the reference to gold. It also incorporated the idea that these proofs were chained together, one after the other, and the last valid proof was used as a challenge.

[22] Adam Back, Hashcash - A Denial of Service Counter-Measure (2002).
[23] Nick Szabo, *Bit gold* (2008).

The problem faced by all digital currency projects was what is technically known as the Byzantine Generals Problem.[24] "Briefly, the problem consists of trying to agree on a course of action or the state of a system by exchanging information over an unreliable and potentially compromised network."[25] In this case, the plan of action is a secure payment system, i.e., where there is no fraud.

The solution Nakamoto found with Bitcoin was to combine:[26]

1. The Back hashcash algorithm as a consensus mechanism with a shared peer-to-peer [P2P] (distributed) database.

2. The Szabo transaction chaining.

3. The public key system serves as a guarantor of ownership, as seen in Dai's b-money.

The result of this combination is as follows: a type of agent called a miner solves these proofs of work to create valid blocks. A series of transactions is put together in these blocks, each cryptographically linked to the previous and next block. Because they are linked in this way, altering one block also requires changing all the subsequent blocks in the chain. The chain of valid blocks is shared in a peer-to-peer (P2P) network, so no central authority keeps track of transactions. At each block, new bitcoins are created and circulated. Transactions are messages in which one address sends a certain number of bitcoins to another, and the messages are signed with the private key corresponding to that address. Any computer can participate in the system as a miner or user; there is no access control.

The document in which he presented this idea was sent by its author to an email list called The Cryptography Mailing List on October 31, 2008.[27] Initially, his project was met with skepticism, and Nakamoto had to defend its viability. That was until one programmer became enthusiastic about the idea. This programmer was Hal Finney, who had already participated in the cypherpunk debates in the previous decade, particularly regarding the problem of double spending in digital payment systems.[28]

[24] Leslie Lamport, R. Shostak and M. Pease, *The Byzantine Generals Problem* (1981).
[25] Antonopoulos, "Chapter 10: Introduction; History of Bitcoin" In *Mastering Bitcoin: Programming the Open Blockchain.*
[26] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008).
[27] Satoshi Nakamoto, *Bitcoin P2P e-cash paper* (2008).
[28] Hal Finney, *Detecting Double Spending* (1993).

In January 2009, Nakamoto presented the first version of the Bitcoin software. The first block on the chain, known as the genesis block, is dated January 3, 2009, i.e., five days before the software release. This block contains, in the form of a condemnation of the banking system, the headline of that day's Times newspaper in the scriptsig parameter of the coinbase transaction.[29]

```
00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;£íýz{.²zÇ,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.È.ˆŠĀQ2Ÿ:¸ª
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)«_Iÿÿ...¬+|
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 ................
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D ......ÿÿÿÿM.ÿÿ..
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksÿÿÿÿ..ò.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *....CA.Šgý°þUH'
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gñ¦q0·.\Ö¨(à9.¦
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybàê.aÞ¶Iö¼?Lï8Ä
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 óU.å.Á.Þ\8M÷º..W
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 ŠLp+kñ._¬....
```

This parameter (highlighted) has a hexadecimal value of:

```
04FFFF001D0104455468652054696D65732030332F4A616E2F32303039204368616E63656
C6C6F72206F6E206272696E6B206F66207365636F6E64206261696C6F757420666F722062
616E6B73
```

When encoded in ASCII, it can be read as:

```
ÿÿÿÿM.ÿÿ....EThe Times 03/ Jan/2009 Chancellor on brink of second
bailout for banks
```

The headline of the newspaper referred to is:

> Chancellor on Brink of Second Bailout for Banks[30]

[29] For technical details, see Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*.

[30] Frances Elliott and G ary Duncan, "Chancellor Alistair Darling on Brink of Second Bailout for Banks," The Times (2009).

From then on, Nakamoto and Finney continued working on the software on a separate e-mail list called bitcoin-list and on the Bitcoin Forum, after a brief stint in the P2P Foundation forum.[31]

Finney passed away in August 2014, and Nakamoto eventually stopped participating in Bitcoin development. His last message was that "he had moved on to other things and that the project was in good hands."[32]

But how, having started from that impasse, did it go from being an experiment among certain anonymous Internet users to being a valid medium of exchange in transactions equivalent to millions of US dollars? A particularly significant event in this regard is Bitcoin Pizza Day. This name commemorates the first recorded transaction in which some goods were purchased using bitcoins.[33] The product in question is, of course, pizza —two pizzas, not just one. That transaction occurred on May 22, 2010, and the buyer paid 10,000 bitcoins for those two pizzas. That price would be ridiculously high today since entire pizza production and distribution chains can be bought with that amount. In any case, and as paradoxical as it may sound, if he had not spent those ten thousand coins, perhaps they would not have reached that value today.

In short, the origin of cryptocurrencies is voluntary and intentional, unlike most of the currency commodities studied by Einzig, just as is the case with legal tender and social currencies. Its origin cannot be found in a previous non-monetary use, religious, symbolic, matrimonial, political, ornamental, nor from barter, nor by internal or external exchange.[34] Its origin is that of an experiment or digital toy that progressively acquired more 'serious' use cases.

Figure 12: Bitcoin graphical representation.

[31] Satoshi Nakamoto, Bitcoin Open Source Implementation of P2P Currency (2009).

[32] Mike Hearn, *Re: Could Satoshi come back and tell us what he/her thinks about the block size?* (2013).

[33] laszlo, *Pizza for bitcoins?* (2010).

[34] While there are political intentions in the creation of Bitcoin, the political origin of the currency referred to by Einzig is that of a good that in the first instance is requested as tribute or political payment by an authority.

◆ Value

One of Bitcoin's most interesting and contentious aspects is its value, a topic that is already a subject of debate in economic science. This subsection comprises four chapters, in which I will explain Bitcoin from the perspectives of different theories of value and assess their usefulness in explaining it.

There are certain commonplaces within the Bitcoin community regarding this matter, a few of which contradict each other. On the one hand, it is argued that the proof-of-work mechanism endows Bitcoin with intrinsic value (*bonitas intrinseca*); in contrast to legal tender, whose value is purely nominal (*valor impositus*). To assume this would be to ascribe to the classical labor-value theory, which most Bitcoiners also disavow as belonging to Marxist thought. In parallel, it is often argued that Bitcoin is a commodity and, therefore, its exchange value is derived from its use value. As Mises concluded, this use value must be exclusively related to its utility as a medium of exchange and not with a prior use value.

In this work, I have already presented how this theoretical difficulty regarding the essence of currency and money can be overcome, following Moini's theory. However, the value question is still susceptible to in-depth analysis, beyond the implications it may or may not have for making Bitcoin a valid monetary instrument, better or worse. For this, it is necessary to adopt the perspective that Moini points out as individual and view Bitcoin as a good, thereby observing what qualities provide it with value to that individual. However, it is not because it is good that it became a medium of exchange; rather, it is the other way around.

Cost of production

The Cost of Production theory derives from the labor-value theory, developed by the classical economists, and continued by Marx, who understands money in this manner:

> It is because all commodities, as values, are realised human labour, and therefore commensurable, that their values can be measured by one and the same special commodity, and the latter be converted into the common measure of their values, i.e., into money.[35]

[35] Marx, *Capital: A Critique of Political Economy*, Volume One, 67.

Currency is, in principle, one more commodity among others and acquires its value according to the labor required to produce it. The exchange value of commodities is given by the proportion between the labor needed to produce that specific commodity and the commodity that fulfills the monetary function. The Bitcoin community ascribes to this theory to contrast the cryptocurrency with legal tender currencies,[36] which obtain their value by force of law and not by their intrinsic qualities. The production process of cryptocurrencies is mining, at least of the proof-of-work ones.[37]

The proof of work consists of finding a valid hash for the header of the new block. A hash is a bit string or value of an arbitrary size, generated by processing a bit string of any size in a hash function; that is, a hash function converts a bit string of any size into one of a specific size. In the case of the block header, the function is SHA-256 and produces a 256-bit hash from a bit string consisting of the following elements, whose size is 80 bytes or 6400 bits:

Table 6: Elements that make up the header of a Bitcoin block. Source: Bitcoin Wiki. Also, in Antonopoulos.[38]

Size	**Field**	**Description**
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the Merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (in seconds elapsed since Unix Epoch)
4 bytes	Difficulty Target	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

> Bitcoin mining uses the hashcash proof-of-work function; the hashcash algorithm requires the following parameters: a service string, a nonce, and a counter. In bitcoin the service string is encoded in the

[36]Noel Jones, "The Intrinsic Value of Bitcoin," *Bitcoin Theory*, (2013).
[37]Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (2008): 3.
[38]Antonopoulos, "Chapter 9" *In Mastering Bitcoin: Programming the Open Blockchain.*

> block header data structure, and includes a version field, the hash of the previous block, the root hash of the Merkle tree of all transactions in the block, the current time, and the difficulty. Bitcoin stores the nonce in the extraNonce field which is part of the coinbase transaction, which is stored as the left most leaf node in the Merkle tree (the coinbase is the special first transaction in the block). The counter parameter is small at 32-bits so each time it wraps the extraNonce field must be incremented (or otherwise changed) to avoid repeating work. (…) When mining bitcoin, the hashcash algorithm repeatedly hashes the block header while incrementing the counter & extraNonce fields.[39]

The hash is a 256-bit string:

1010111000110111001101000011101000110101011110101000001010010111010110010
0010110001001011110011100010011010011001011111010100010001011110101100100
1010001011111010001100101000101010001100101010101001000111010111001111000
0010111111101010000100110011010110111

It is represented by alphanumeric characters:

ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7

In turn, it can be read as a hexadecimal number and translated to decimal:

787999727021700517185438783376474198024680928389279738726171287656394592355511

Therefore, the hash is a numeric value that can be greater or less than another number.

To be valid, the block's hash must be less than the network's target. Miners compete to find a valid hash and collect the reward. This reward comprises the fees (which users pay to make each transaction) and the coinbase reward (new coins created in each block).

To summarize, the Bitcoin production process works as follows: miners work by generating several hashes until they find one that meets the validity criteria; when this is achieved, a new block is added to the chain, and the miner who produced it is awarded the reward contained in this new valid block. A user who wants to make a Bitcoin transaction generally pays the miners a fee to settle their transaction. The economic product of the miners' work is new coins (a good) and the functioning of the payment system (a service). The benefit they receive is bitcoins: those created in the mining process and those paid by users.

[39] Bitcoin Wiki, "Block Hashing Algorithm."

Now that the productive process in Bitcoin is explained, it is time to evaluate how it gives value (or not) to the currency. The fundamental premise of the labor-value theory is that "The real price of everything, what everything really costs to the man who wants to acquire it, is the toil and trouble of acquiring it."[40] Following this principle, the value of Bitcoin would vary in inverse proportion to the total amount of hash power used to produce new blocks, as it would be less expensive and therefore worth less. Figures 13 and 14 compare the evolution of network mining power, price, and market capitalization from 2014 to 2019. While initially both lines coincide, by 2017 the divergence is clear.

Figure 13. Bitcoin price evolution in the period 2014-2019. Source: "https://coinmarketcap.com/currencies/bitcoin/"CoinMarketCap

[40]Smith, *An Inquiry Into the Nature and Causes of the Wealth of Nations*, 50.

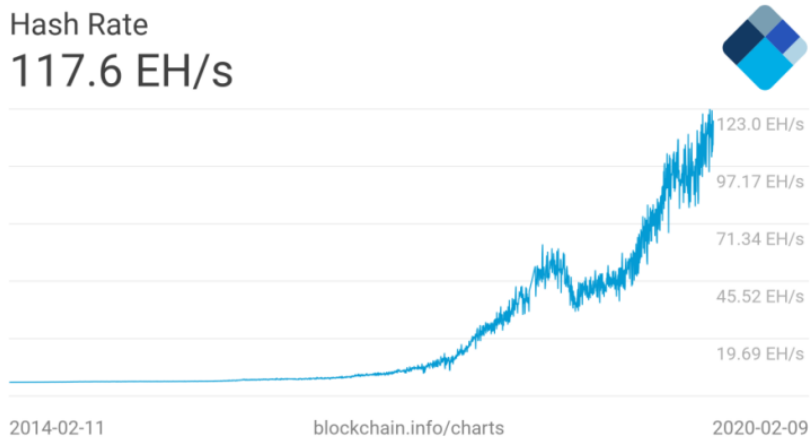


Figure 14. Evolution of Bitcoin network mining power in the period 2014-2019. Source: "https://www.blockchain.com/charts/hash-rate?timespan=6years" blockchain.com

I will pose the following hypothetical scenario: the block reward is 25 bitcoins, and a miner works alone with a hash power of 100 H/s. With that mining power, he solves a block every 10 minutes since he needs to try approximately 60,000 hashes until he gets the right one. If this miner doubled his mining power to 200 H/s, reaching the solution would only cost him half the time, and he would produce two blocks in 10 minutes, thereby pocketing 50 bitcoins within the same work time.[41] As it costs less work to produce each bitcoin, its price would tend to go down; that is, the price of each bitcoin should be inversely proportional to the mining power. However, when I compare this hypothetical case with the real data, it bears no resemblance whatsoever: Bitcoin was not worth much when mining power was minimal.

[41] I leave aside the transaction fees to simplify the argument.

COUNTRY	COST
Venezuela	$ 531.00
Trinidad and Tobago	$ 1 190.00
Uzbekistan	$ 1 788.00
Ukraine	$ 1 852.00
Kuwait	$ 1 983.00
Myanmar	$ 1 983.00
Belarus	$ 2 177.00
Bangladesh	$ 2 379.00
Kazakhstan	$ 2 835.00
Ethiopia	$ 2 855.00
Suriname	$ 2 956.00
Kosovo	$ 3 133.00
Serbia	$ 3 133.00
Paraguay	$ 3 140.00
China	$ 3 172.00
Egypt	$ 3 172.00
Saudi Arabia	$ 3 172.00
Iran	$ 3 217.00
India	$ 3 274.00
Georgia	$ 3 316.00
Nepal	$ 3 569.00
United Arab Emirates	$ 3 569.00
Zambia	$ 3 569.00
Taiwan	$ 3 774.00
Albania	$ 3 894.00
Macedonia	$ 3 914.00
Canada	$ 3 965.00
Bosnia and Herzegovina	$ 4 084.00
Peru	$ 4 140.00
Indonesia	$ 4 329.00
Bulgaria	$ 4 362.00
Argentina	$ 4 560.00
Moldova	$ 4 651.00
Russia	$ 4 675.00
Vietnam	$ 4 717.00
Iceland	$ 4 746.00
Slovakia	$ 4 746.00
Sweden	$ 4 746.00
Brunei	$ 4 758.00
United States of America	$ 4 758.00

Both values took off starting in 2017, and the price oscillated over the next few years while mining power increased, albeit with some stumbles.

This is due, in principle, to a mechanism I mentioned tangentially: difficulty. If we go back to Table 4, there is a variable that refers to difficulty, the second -to-last, and the target. What I had said about it is that the target determines the validity of a block because the hash must be less than that target to be valid. I also noted in that table that this value changes when the difficulty level changes. Now it is worth noting that the difficulty changes every 2016 blocks,[42] blocks if the time between blocks deviates from ten minutes. To be clear and technically correct: what really changes is the target; the difficulty is a consequence of it. If the target is lower, the difficulty increases, and vice versa. Consequently, the cost of producing a block increases or decreases according to the amount of work that goes into producing blocks.

[42] Bitcoin Wiki. "Difficulty."

Laos	$	4 845.00
Thailand	$	4 943.00
Turkey	$	4 984.00
Malaysia	$	5 147.00
Fiji	$	5 155.00
Lithuania	$	5 155.00
Nigeria	$	5 321.00
Hungary	$	5 365.00
Croatia	$	5 551.00
Estonia	$	5 551.00
Romania	$	5 698.00
Gibraltar	$	5 710.00
Singapore	$	5 936.00
South Africa	$	5 948.00
Feb 2018 Minimo	$	6 048.26
Malta	$	6 079.00
Israel	$	6 087.00
Montenegro	$	6 384.00
Iraq	$	6 543.00
Brazil	$	6 741.00
Poland	$	6 931.00
Finland	$	7 122.00
Latvia	$	7 122.00
Pakistan	$	7 137.00
Philippines	$	7 137.00
Colombia	$	7 157.00
Switzerland	$	7 494.00
New Zealand	$	7 593.00
Uganda	$	7 637.00
Mexico	$	7 645.00
Slovenia	$	7 645.00
Luxembourg	$	7 693.00
Norway	$	7 784.00
Jamaica	$	7 867.00
France	$	7 930.00
Hong Kong	$	7 930.00
Liechtenstein	$	8 164.00
Cambodia	$	8 327.00
United Kingdom	$	8 402.00
Nicaragua	$	8 613.00
Cyprus	$	8 723.00

Keeping blocks separated by a ten-minute interval is a technical necessity related to the distribution of information throughout the network. Experiments on this subject were carried out by Geier[43] from the University of Buenos Aires and are not relevant to this work. Beyond that, this adjustment of the difficulty has an economic effect that I am interested in analyzing: it creates scarcity. A higher mining power does not give the miner a higher production capacity, as in the hypothetical case I mentioned above. Still, it guarantees him a larger portion of the fixed production.

In other words, this mechanism brings as a consequence the fact that the labor value of each block varies: a mining power of 100 H/s is going to take approximately 10 minutes to produce a block, and one of 100 EH/s (10^1 times more) will also take 10 minutes. In the above case, with a single miner taking care of the entire network, it would be more profitable for him to employ as little work as possible and thus be more cost-effective. But the Bitcoin system is open, and, seeing the ease with which this miner is generating money, others will do the same. This increases the network's hashing rate and difficulty, leaving the first miner with only a tiny chance of creating new blocks and earning the reward.

[43] Maximiliano Iván Geier, *Análisis del Comportamiento de Aplicaciones Paralelas y Distribuidas por Medio de Técnicas de Emulación de Redes* (Ph. D Thesis, Universidad de Buenos Aires 2018).

Japan	$	8 723.00
Uruguay	$	8 723.00
Rwanda	$	8 922.00
Palau	$	9 053.00
Chile	$	9 120.00
Greece	$	9 120.00
Netherlands	$	9 449.00
Australia	$	9 913.00
Jordan	$	9 913.00
Papua New Guinea	$	9 913.00
Italy	$	10 310.00
Guyana	$	10 627.00
American Samoa	$	10 706.00
Portugal	$	10 825.00
Ireland	$	11 103.00
Spain	$	11 103.00
Tahiti	$	11 103.00
Sri Lanka	$	11 630.00
Feb 2018 Maximo	$	11 880.14
Curaçao	$	11 896.00
Western Samoa	$	12 689.00
Kiribati	$	12 966.00
Vanuatu	$	13 085.00
Belgium	$	13 482.00
Turks And Caicos Islands	$	14 033.00
Denmark	$	14 275.00
Germany	$	14 275.00
Tuvalu	$	14 493.00
Tonga	$	14 671.00
Marshall Islands	$	14 751.00
Cook Islands	$	15 861.00
Solomon Islands	$	16 209.00
Bahrain	$	16 773.00
Niue	$	17 566.00
South Korea	$	26 170.00

Table 5: Cost of mining 1 unit of bitcoin in different countries updated in February 2018 and bitcoin market prices in the same month. Sources: Elite Fixtures (costs), CoinMarketCap (market price).

So far, we have a system that is very closed within itself and whose operation seems redundant. The cost of producing a block is determined by the work put into producing blocks; producing blocks generates money that circulates, utilizing information inscribed in those same blocks; and all this serves only to transfer those same units that the system produces. It seems that all this is a kind of game or model without any utility; everything begins and ends within the system. Unlike the production of a material object, a bitcoin only exists within the Bitcoin system. Everything starts and ends inside, except the work that the miners are carrying out, which consumes a lot of time and energy, and for what? At this point, what can be considered the use value of Bitcoin comes into play: security.

Given how the blockchain works, to successfully perform a fraud (e.g., reverse a transaction and recover what was spent), an attacker would have to modify the information he wants to alter and all the blocks that follow, one by one, since the header of each block must be derived from that of the previous block. The amount representing this probability of success was detailed by Nakamoto;[44] however, more recently, Dian developed equations using the US dollar values of the inputs and energy required to carry out this attack, arriving at a minimum value of approximately $1,006,247,000 per day.[45] Other sources calculate the estimated cost of this type of attack in real time.[46]

[44]Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 6.

[45]Mario Dian, "Cost of a 51% Attack and Security of Bitcoin, Monero, Litecoin and other Cryptocurrencies" Freedom Node, (n.d.).

[46]GoBitcoin, "Cost of a 51% Attack."

The use value gained from mining is the power to transfer amounts from one address to another and the assurance that those transfers cannot be tampered with. That explains the value of the Bitcoin system as a service but not the value of bitcoins as a commodity that is produced and sold. This occurs because, as can be inferred from the above, there is no direct relationship between the labor employed and the number of bitcoins produced. I already explained how the difficulty setting keeps the production of new coins constant, no matter how much the work put into it varies. Yet, it should also be noted that the reward per block is an entirely arbitrary value. Whether there are 2, 10, 50, or 1,000 bitcoins in a block does not depend on the miners' effort; rather, it is written into the software. Moreover, the bitcoin unit is also arbitrary. Technically, the indivisible unit of the Bitcoin network is not one bitcoin but 1 Satoshi, equivalent to 0.00000001 bitcoin.

The labor invested in Bitcoin, then, is not directly crystallized in the monetary units as in any commodity-currency. Although the monetary units share a certain similarity or homogeneity, each one requires a specific investment of labor, and in that sense, their values are independent of one another. In Bitcoin, the labor value is condensed into the global hash rate, and from there, it is divided into the existing units that express it as exchange value.

However, there is one more element to mention: a part of the mining process that does incur a direct valorization of labor: fees. When someone makes a transaction, he writes it in a new block, and to do that he pays a fee to the miners, which is optional (it can be zero or more, and that is decided by the one who makes the transaction). A transaction contains certain information, including the input and output UTXOs (Unspent Transaction Outputs) and the signatures that validate it.[47] This information has a certain size in bytes, and each block has a size between 1 MB and 1.3 MB on average nowadays,[48] but its maximum is 4 MB since the implementation of SegWit.[49] The transactions are sent to the mempool or memory stack, where the miners choose some of them and make a new block. The fee is used to incentivize miners to include the transaction and be able to collect

[47]This concept will be explained in more detail in the "Portability" chapter of the "Properties" section. See also: Antonopoulos, "Chapter 6" In *Mastering Bitcoin: Programming the Open Blockchain*.

[48]For more information, see Blockchain.com "Average Block Size."

[49]Bitcoin Wiki, "Block size limit controversy"

it. It is calculated as an amount of satoshis per byte, given that what is in dispute is a scarce space within a block that miners must then process into a hash.

This is how this fee mechanism directly values the work of mining. However, the fees are still too small relative to the block reward, which is the miners' primary source of income. Eventually, this relationship will reverse, as successive cuts in half (halvings) of the block reward cause it to fall below the average fee.

Next, I will examine the geographic distribution and the amount miners can earn.

Table 5 presents the costs of producing one unit of bitcoin and its market value during February 2018, the month when the research used as a source was conducted. The countries colored in red are those that had a higher production cost than the maximum market price reached in that period, so it was not profitable to produce; the orange ones are those that had intermediate costs between the maximum and minimum prices, i.e., it was at times profitable or approximately it would have reported neither profit nor loss to mine. The countries colored green always had a production cost below the market price, so it was profitable to mine there. On the other hand, Figure 16 shows a map showing the distribution of mining industries around the world.

Following the most logical reasoning, the countries with the highest mining activity are in the most profitable spectrum of the Table: China, the United States, Canada, Iceland, Sweden, and Russia. Leaving aside the extreme case of Venezuela, where the cost of mining is minimal, but the political climate was hostile to miners,[50] most miners were producing at a cost of between USD 4,000 and USD 4,800 per coin, when the coin was sold at a minimum of USD 6,000 and a maximum of USD 11,900. In other words, it has a profit margin between 50% and almost 200%. The price of bitcoins is not close to their production cost, because if it were, it would not be so volatile, since production costs do not vary so abruptly. What determines the cost of production is a minimum price, a support below which it is difficult for the price to fall.

[50]Luis Esparragoza, "Mineros Venezolanos Apagan sus Equipos por Temor a Persecución Policial," *Criptonoticias* (2017).

Figure 15. Global overview of Bitcoin mining regions. Regions with relevant large-scale miners shown in cyan, Sichuan in dark blue and remaining small-scale regions in black.[51]

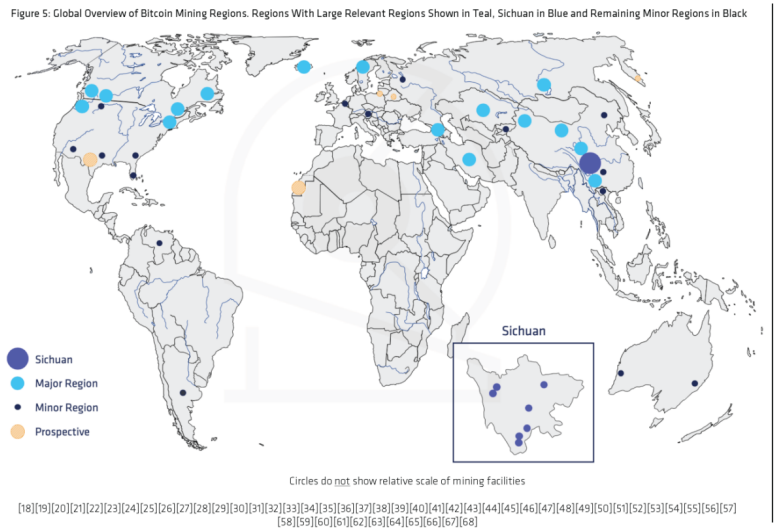
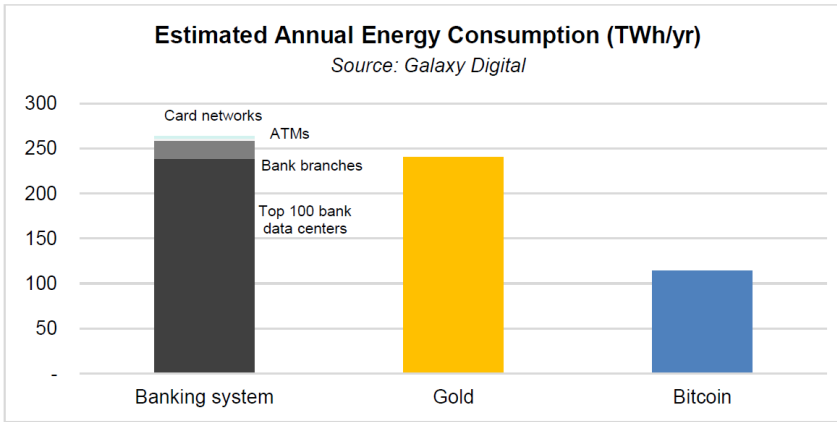


Figure 5: Global Overview of Bitcoin Mining Regions. Regions With Large Relevant Regions Shown in Teal, Sichuan in Blue and Remaining Minor Regions in Black
3 December 2019
7
Sichuan
Sichuan
Major Region
Minor Region
Prospective
Circles do not show relative scale of mining facilities
[18][19][20][21][22][23][24][25][26][27][28][29][30][31][32][33][34][35][36][37][38][39][40][41][42][43][44][45][46][47][48][49][50][51][52][53][54][55][56][57]
[58][59][60][61][62][63][64][65][66][67][68]

Figure 16. Estimated annual energy consumption (TWh/year) compared between Bitcoin mining, the gold industry, and the banking system.[52]On the Bitcoin energy consumption debate.[53]



[51]Christopher Bendiksen and Samuel Gibbons, The Bitcoin Mining Network. Trends, Composition, Average Creation Cost, Electricity Consumption & Sources (2018), 20.

We can shift the focus from this machine work to the human work that goes into programming Bitcoin and other cryptocurrencies, namely, software development work. For this, I will use a report from 2019 by a venture capital firm that tracks and compares the development teams of various cryptocurrency projects.[54]

Figure 17: Evolution of the net number of developers of different cryptocurrencies.

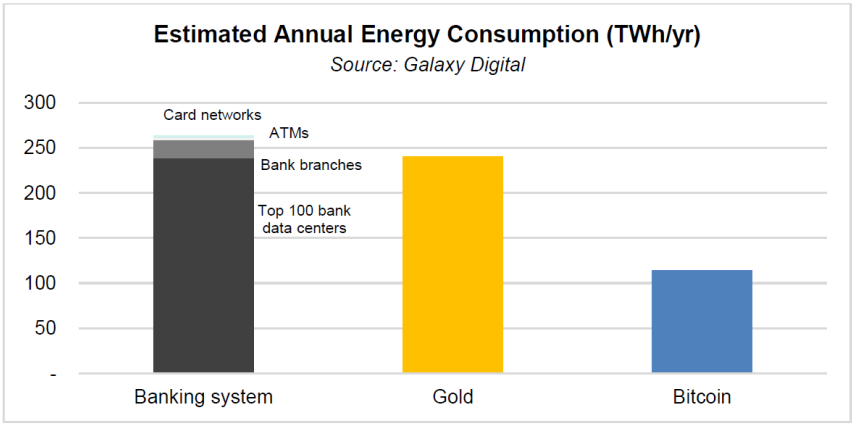
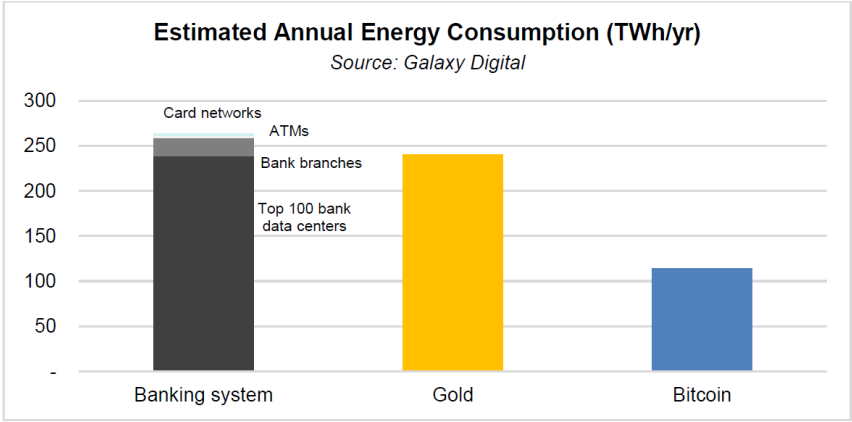


Figure 18: Number of developers (x-axis) versus network value (y-axis).



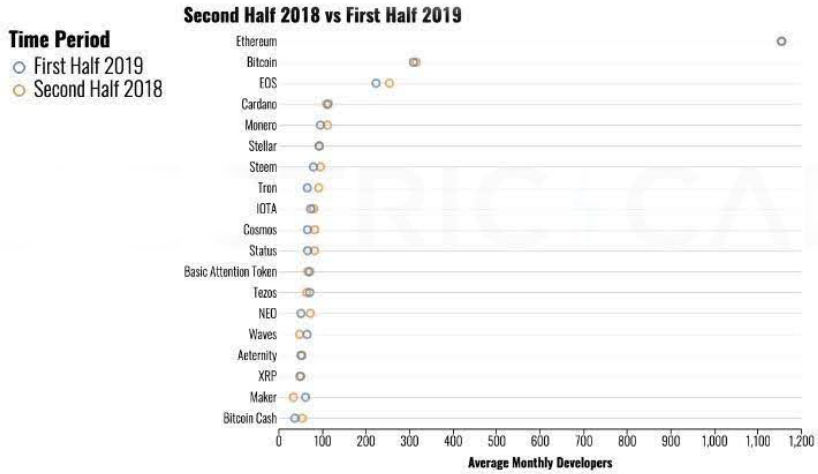
[52]Rachel Rybarczy, Drew Armstrong, and Amanda Fabiano, *On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question* (2021), 13.

[53]E. Faria, *Bitcoin Energy Consumption Debunked* (2021).

[54]Electric Capital, "Electric Capital Developer Report (H1 2019)," *Medium*, (2019)

As can be seen in the Figures above, Ethereum has the network with the largest number of developers. However, its market value is far below that of Bitcoin, with far fewer developers working, and not far behind that of most cryptocurrencies, with little value and few developers.

Figure 19: Top 19 cryptocurrencies with the largest number of developers working on them.
19 of Top 100 ecosystems averaged 40+ monthly developers



Electric Capital

The values in Figure 20 can be compared with those in Figure 33 (in the chapter "Measure of Value or Unit of Account"), which contains a similar graph but with values representing market value rather than the number of developers. I can compare the first five of each figure to note how little correlation there is between one value and the other:

Table 7: Top five ranking of cryptocurrencies by quantity of developers and market capitalization.

Position	Developers	Market Cap.
1	Ethereum	Bitcoin
2	Bitcoin	Ethereum
3	EOS	Tether
4	Cardano	XRP
5	Monero	Bitcoin Cash

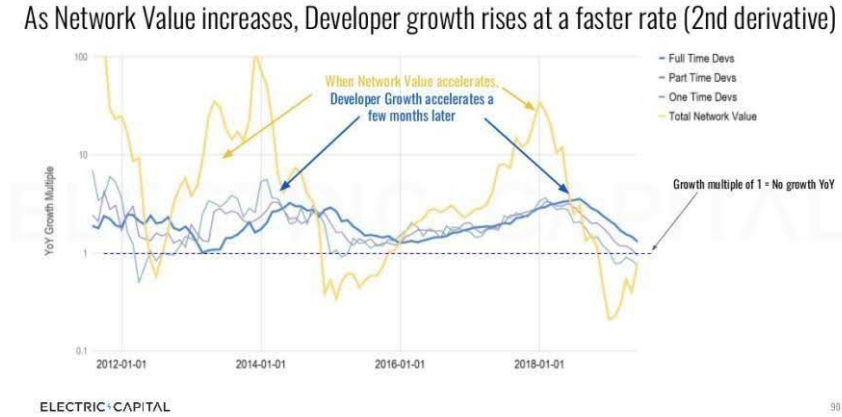


Figure 20: Comparative growth in the number of developers and the value of the network.

In a more recent paper, a team from several European universities studied the linkages between development teams (developers working on multiple projects) and the correlations between these linkages and the market prices of the projects. They came to similar but not quite identical conclusions:

> The Ether community soars above the others in terms of editing activity (109, 527 development events), while Bitcoin has the largest number of developers, 832;[55]

[55]Lorenzo Lucchini, L. Alessandretti, B. Lepri, et al., "From Code to Market: Network of Developers and Correlated Returns of Cryptocurrencies," (2020): 4.

> for months after the GitHub connection time, the correlation between the return time series of two GitHub-linked cryptocurrencies increased, on average.
>
> …other market indicators - and in particular volume - do not show the same behaviour.
>
> Finally, we showed that developers tend to work on an established currency first and that linked pairs containing at least one top cryptocurrency exhibited a larger correlation of returns following connection.[56]

Nor does this more background and long-term work seem to explain Bitcoin's value. This is not an atypical phenomenon in the case of currencies, since Einzig says in this regard:

> It would be very difficult (…) to establish any strict arithmetical relationship between the cost of production of these and other primitive currencies and their value. In some instances some such relationship appears to be noticeable. (…) On the other hand, there are many instances of wide discrepancies between the cost of production and the value of primitive money.[57]

Supply, demand, quality, and quantity

The usual way to quantitatively measure the value of Bitcoin is by its market price, which is its exchange value, but this value is highly volatile. The reference price in retail transactions, in wallet software and on dedicated crypto-economy platforms comes from Bitstamp, CoinMarketCap, Coin Gecko or Coincap. Bitstamp is a cryptocurrency exchange itself, whose price the community takes as a direct reference. At the same time, the other platforms are dedicated to building averages and indexes from multiple cryptocurrency exchanges or markets, such as Binance, Huobi, Kraken, Bitfinex, Bithumb, Bittrex or Coinbase Pro, to name the most popular ones. CoinMarketCap lists a total of 20,386 pairs for 10,089 cryptocurrencies at the time of this writing; Coincap: 1,518 coins, 5,063 pairs in 71 markets; and Coin Gecko: 6694 currencies in 405 marketplaces.

This information is more accurate than the one I discussed in the previous section, but not always more transparent, since ultimately, the exchanges or markets publish the data on their own activity. All information

[56] Ibid., 7–8.

[57] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 406.

goes through their servers (except for decentralized exchanges, or DEX, which operate on proprietary blockchains but are less critical in terms of volume). Several controversies have arisen regarding manipulations in the volumes and prices reported by both markets and indices.[58]

In comparison to other forms of currency, this is the aspect in which Bitcoin differs the most. The current and maximum possible supply of bitcoins are always publicly known. The number of bitcoins in circulation is estimated, a point I will explain in the next chapter. In the case of paper money, the amount issued by a central bank is known, but not the actual monetary base; and in the case of commodity-currency, the circulating currency is only known in closed, small-scale systems such as Rossel Island. More importantly, the bitcoin circulating supply has a limit to which it can grow and, although its monetary base grows constantly due to the mining process, that growth is reduced to 50% every 210,000 blocks;[59] which, added to eventual coin losses, means that in the long run the monetary base tends to become smaller and smaller.

According to the quantity theory:

> …prices vary directly with the quantity of money in circulation, provided the velocity of circulation of that money and the volume of trade which it is obliged to perform are not changed.[60]

If this assumption is followed, the price of Bitcoin should progressively increase over time, if the velocity of circulation and the volume of exchange remain the same or increase.

> BOTH the nominalist school and the commodity school of monetary theorists agree that the quantity of money is liable to affect its value. They arrived at this conclusion, however, through totally different lines of approach. According to the commodity theory, money is like any other commodity and its value is therefore naturally affected by supply and demand. According to the nominalist school, money has no intrinsic value, it is merely an abstract claim on commodities in general, and the total volume of claims determine the purchasing power of a unit. The result of the difference between the two lines of approach is that while the nominalists believe in the quantity theory

[58]John M. Griffin and Amim Shams, "Is Bitcoin Really Un-Tethered?," Soc. Sci. Res. Netw. (2019) 119.

[59]Antonopoulos, "Chapter 10," In *Mastering Bitcoin: Programming the Open Blockchain*.

[60]Irving Fisher, *The Purchasing Power Of Money: its Determination and Relation to Credit Interest and Crisis* (The Macmillan Company, 1922): 14.

> of money, the commodity theorists believe in the supply and demand theory. The difference between the two theories is largely one of emphasis and method of approach. The quantity theory allows not only for the volume of money and the volume of goods, but also for the velocity of circulation of money. Even this difference is largely one of form rather than of substance; for, after all, the active supply of money is determined by two factors: its quantity and the velocity of its circulation.[61]

However, referring to the quantity of bitcoins is also problematic. Being immaterial, their quantity is in principle irrelevant, since storing and transferring any amount is just as costly, unlike with material currencies. This is nothing new, as digital means of payment have existed long before cryptocurrencies. The novelty is, on the one hand, the autonomy of the system, which does not depend on backing in something else, but its units are worth by themselves; on the other hand, the immense divisibility of these units. This second factor is of tremendous importance since it makes a shortage of circulating currency virtually impossible. If a large part, even the majority, of the bitcoins in existence were to be immobilized for some reason, the little liquid circulating currency would be capable of covering all the demand for volume and speed in a short time, without the need to create more coins, but only by further subdividing and valuing those that remained in circulation, as Wicksell already commented on his ideal banking system.

On the other hand, the qualitative theory is the metallic paradigm, in which a good that serves as a monetary instrument must have a prior intrinsic value.[62] As I explained in the previous chapter, bitcoins do not have an intrinsic value based on how much work it costs to produce them, because there is no strict relationship between the work employed and the bitcoins produced. However, they do have intrinsic value as a payment system. Ethnographically, it has been observed that:

> …the intrinsic value of primitive currencies is not always represented by their commodity value. Often it is a prestige value, or sentimental value, or religious value. Such currencies cannot be described as commodities, but so long as they possess a value that is not derived from their monetary use, they may be said to have intrinsic value.[63]

[61] Einzig, Primitive Money in its Ethnological, Historical and Economic Aspects, 391.
[62] Ibid., 401.
[63] Ibid., 401.

Bitcoin cannot be said to have a non-monetary value, which raises questions about whether it is a commodity currency. Starting from the fundamental distinction between use-value and exchange-value, the monetary instrument finds itself in a paradox, as we have already seen: its use-value is to be exchange-value.

As Godelier documented, the labor-value or cost of production is only mentioned in the last instance of negotiation as a floor for the price or exchange-value. In the first place, and as a ceiling, use-value or utility, as pointed out by the marginalist school, utility and labor can be considered, in a word, as two sides of the same coin. To develop this point, it is helpful to begin by quoting the definitions of both measures.

- Labor-value, from Smith:
  The real price of everything, what everything really costs to the man who wants to acquire it, is the toil and trouble of acquiring it. What everything is really worth to the man who has acquired it, and who wants to dispose of it or exchange it for something else, is the toil and trouble which it can save to himself, and which it can impose upon other people. What is bought with money or with goods is purchased by labour as much as what we acquire by the toil of our own body. That money or those goods indeed save us this toil. They contain the value of a certain quantity of labour which we exchange for what is supposed at the time to contain the value of an equal quantity.[64]

- Utility-value, from Menger:
  Things that can be placed in a causal connection with the satisfaction of human needs we term *useful things.*1 If, however, we both recognize this causal connection, and have the power actually to direct the useful things to the satisfaction of our needs, we call them *goods.*[65]

  The satisfaction of some one human need is therefore dependent on the availability of each concrete, practically significant, quantity of all goods subject to this quantitative relationship. (...) The value of goods, accordingly, is a phenomenon that springs from the same source as the economic character of goods—that is, from the rela-

[64]Smith, *An Inquiry Into the Nature and Causes of the Wealth of Nations*, 50–51.
[65]Carl Menger, *Principles of Economics*, (Auburn University Press, 2007): 52.

> tionship, explained earlier, between requirements for and available quantities of goods.[66]

Although they are considered opposing views, labor-value and utility-value are perfectly compatible. Note the caveat that Smith makes in his definition: labor value appears when the producer does not intend to consume his own product; that is, when for him, utility is exhausted, and he has a surplus. From this point of view, to work (from the Latin *tripaliāre*, to torture) is to engage in an unsatisfactory activity to obtain future satisfaction, which is known as the "cost/benefit equation" and the reason why in a self-sufficient economy one stops working as soon as one has enough to satisfy one's needs.[67] Mises also devotes a few paragraphs to raising this question about the "prosumer":

> In an isolated household, in which (as on Robinson Crusoe's desert island) there is neither buying nor selling, changes in the stocks of goods of higher and lower orders do nevertheless occur whenever anything is produced or consumed; and these changes must be based upon valuations if their returns are to exceed the outlay they involve. (…) the calculation whether a certain act of production would justify a certain outlay of goods and labour is exactly the same as the comparison between the values of the commodities to be surrendered and the values of the commodities to be acquired that must precede an exchange transaction.[68]

In a market economy with the division of labor, production and consumption are carried out by different agents, but the calculation works similarly. Thus, we have a labor-value on the supply side: the minimum that the producer is willing to accept as satisfaction for his effort; and on the other hand, on the demand side, the utility-value: the maximum that a consumer is willing to pay for the utility of the commodity.[69] We can thus see utility (satisfaction) and labor (dissatisfaction) as two concepts that refer to the same magnitude, but in opposite ways. Just as 'cold' is technically 'less heat', yet this magnitude is referred to as if it were a positive value: 'it is very cold'; we can say that labor is less satisfying and vice versa.

[66] Ibid., 115.
[67] A.V. Chayanov, *The Theory of Peasant Economy*, (Richard D. Irwin, 1966).
[68] Mises, *The Theory of Money and Credit*, 38–39.
[69] Whether needs or work are in themselves objective or subjective is a subject that has given rise to enormous controversy and is beyond the scope of this study.

In conclusion, due to the extreme relativity of the production cost of bitcoins, as explained in the previous chapter, their value is derived, to a greater extent than most goods, from their utility, specifically the ability to transfer value reliably. This seems redundant or paradoxical, as I am claiming that value depends on the ability to transfer value. But the evidence shows that this is a common case for many monetary instruments:

> From the point of view of the quality theory of money there seems to be no fundamental difference between primitive and modern money. In both cases the theory only holds good in part of the instances. In other instances currencies have no full intrinsic value, if indeed they have any at all. It is not even possible to ascertain any definite trend in monetary history indicating an increase or decrease of the fiduciary character of money in the course of the progress of civilization. Communities in the most diverse stage of civilization used currencies with or without full intrinsic value. Nevertheless, the quality theory is undoubtedly valid as a broad rule in a large proportion of instances.[70]

From the moment in which storing and/or transferring value becomes a necessity, the object (or in this case an abstract accounting system, but with finite units) which can fulfill this function, i.e., the monetary instrument, acquires a utility and therefore becomes a good from the individual point of view, as Menger and Moini explain. It is not necessary to go back to an original moment in which the medium of exchange was just another commodity among others, with a different use value.

[70] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 404.

Extent of use and restrictions

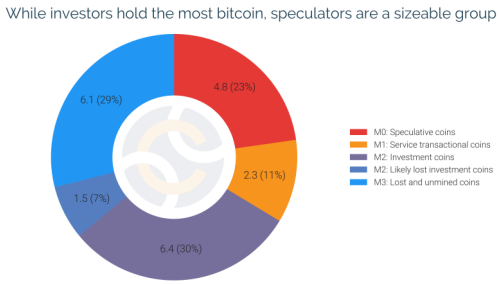


Figure 21: Distribution of Bitcoin's monetary supply (2018)

Currency, seen from the state theory, is universally accepted, at least within the territorial boundaries of a particular nation-state. However, this is not the case for other forms of money. Regarding this variable of a currency's value, Einzig states that,

> THE limitation of the use of a currency tends to affect its value unfavorably. As a general rule, the more restricted the use of a primitive money, the smaller its surplus value in excess of its intrinsic value arising from its monetary use.[71]

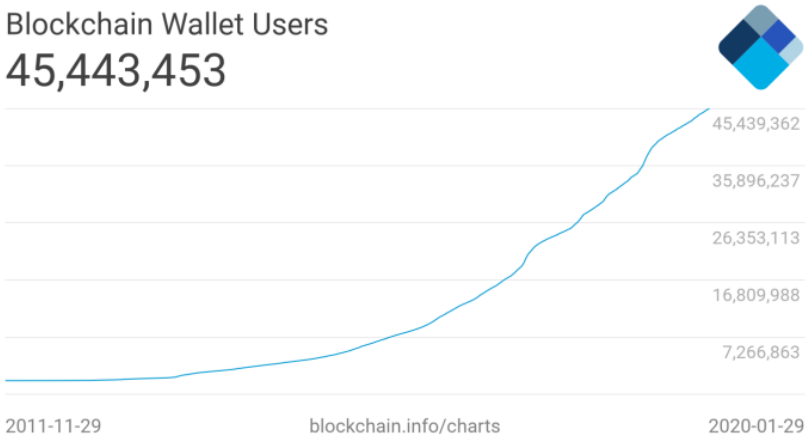


Figure 22. Source: "https://www.blockchain.com/charts/my-wallet-n-users?timespan=all"Blockchain.com. Retrieved on 2020/01/30 at 11:00 hs.

[71] Ibid., 424.

The cryptocurrency community, researchers, and journalists recognize the importance of this, but are unable to quantify it accurately.[72] The very technology and ideology underpinning Bitcoin make it challenging to calculate the extent or limits of its commercial use. All the blockchain shows are transactions between Bitcoin addresses. What one party gave to the other in exchange for those bitcoins is not information that the software can know. Whether the sender and recipient addresses belong to the same person cannot be known from the blockchain either. All this information has to be obtained by other means, so it is up to the traders themselves to declare how much merchandise they trade in bitcoins in order to know the volume of trade in these currencies. What is openly published are the offers of products in exchange for cryptocurrencies, so it is possible to know at least what Bitcoin can buy without knowing the exact value.[73]

Another measure of the Bitcoin market's size is the number of active addresses. This indicator can be misleading, or at least inaccurate, because one address does not necessarily equal one user. This is because a wallet is, in principle, a digital file containing a list of private keys;[74] a private key is "a 256-bit number, which can be represented in one of several ways."[75] From each of these private keys, a corresponding 256-bit public key is mathematically derived. The address that sends and receives bitcoins openly on the network is a 160-bit hash of that public key.[76] A single user can generate several wallets, each with several keys and addresses that seen 'from the outside' (looking only at the public data of the blockchain) have no relation and, conversely, a single address (for example 3M6UcBNGZAW1HRjiFDMRcY5aXFrQ4F9E1y) can contain money from several users because it belongs to a company that holds the funds of its customers. These companies possess detailed information about their users, which can be used to estimate the total usage of Bitcoin and other cryptocurrencies.

With the extent of use of a given currency, Einzig also notes that "The use of an object as a medium of exchange or as a store of value tends to raise its value to a much larger degree [than its use as a standard of de-

[72]See, for example: Juan Ibarra, "Informe: Bitcoin Seguirá Ganando en Adopción Sobre otras Criptomonedas en 2020," *Criptonoticias* (2020).

[73]See Jai Pratap, "What Can You Buy with Bitcoin?," Coinnounce (2019).

[74]Bitcoin.org, "Wallet."

[75]Bitcoin Wiki, "Private Key."

[76]Antonopoulos, "Chapter 4" In M*astering Bitcoin: Programming the Open Blockchain.*

ferred payments]."[77] The use of Bitcoin as a form of value storage is one of the most widespread, if not the most pervasive. Two popular terms in the Bitcoin community account for this: *HODL,*[78] which is an incorrect spelling of hold, and which refers to never selling bitcoin savings. It was popularized informally through memes, jokes, and pranks. On the other hand, in presumably more serious contexts, people talk about "Bitcoin as digital gold"[79] and draw a few analogies between this digital payment system and the precious metal. This type of use, which involves obtaining and storing bitcoins in a wallet for extended periods, also has implications for the information that can be gleaned from the blockchain. The "lost" coins are supposed to be in wallets whose key nobody knows, either because the owner lost it or because they were sent to an incorrect but valid address whose key has yet to be discovered. This can be misleading, as it is not possible to determine, except in rare cases, whether someone has the private key that corresponds to a specific address. In other words, many apparently lost coins may only be resting in the wallets of very long-term savers.

Conversely, it is the case that "the more restricted the use of a primitive money, the smaller its surplus value over its intrinsic value arising from its monetary use." Bitcoin has several factors that limit its usefulness, both internally and externally.

First, I will refer to what is known as scalability.[80] As I explained in the chapter on cost of production, transactions on the network are validated by entering a block with a limited space and a waiting time of about ten minutes. This implies that each transaction will take approximately ten minutes to complete, and the time may increase or the price may rise if there are many pending transactions.[81] This limitation makes Bitcoin impractical for everyday use, known as micropayments, but it is still extremely useful for moving large sums over long distances or between jurisdictions.[82]

[77]Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 425.

[78]Jake Frankenfield, "Hodl"' Investopedia, (2019).

[79]Peter Chawaga, "BTC Bullion: Three Interpretations of Bitcoin as 'Digital Gold,'" *Bitcoin Magazine*, (2019).

[80]Wikimedia Foundation, "Bitcoin Scalability Problem."

[81]Statistics relating to the mempool can be found at Jochen Hoenicke, *Johoe's Bitcoin Mempool Size Statistics* (n.d.) Or in https://mempool.space/.

[82]Kyle Torpey, "Bitcoin is Now Useless for Micropayments, But Solutions are Coming," *Bitcoin Magazine.* (2017).

The second problem, which is partly internal and partly external, is that of fungibility. Since the blockchain is a public database that contains all transactions made by users, cross-referencing this information with external data about the identities of those users allows for tracing the routing of a certain amount of money and the trade links between different actors who utilize the Bitcoin system. This information means that all currencies are no longer equivalent to each other, but there are 'clean' currencies (not associated with any illicit activity) and 'dirty' currencies. This brings into play a theoretical premise of what a monetary system implies: the concept of fungibility. However, it is unclear how significant the individualization of some currencies is for the overall system in practice.[83] This issue will be dealt with in greater depth in a later chapter. To provide a counterexample, consider the case of Rosell, cited in the chapter on ethnographic approaches, where every coin in circulation was known to all individuals participating in the monetary system. There was no exact exchange rate between coins of one value and another. The system as a whole was still operational.

The third problem I will address is purely external to the Bitcoin system and concerns the legal impediments to its use. Countries such as Bolivia, Ecuador, Nepal, Egypt, and Morocco strictly prohibit the use, purchase, and sale of cryptocurrencies on their territory. This should negatively affect the value of cryptocurrencies in these countries, but this is not what happens empirically. At the time of writing, Bitcoin is sold in Egypt for EGP 156,528.03 to EGP 243,971.28, which, with a dollar at 15.64, equates to between USD 10,008.19 and USD 15,599.19. In Bolivia, it is sold between BOB 68,316.83 and BOB 106,020.29, which is equivalent to USD 9,886.66 and USD 15,343.02, respectively, with an exchange rate of 6.91. The price of Bitcoin in dollars at the time of writing is $9,587.99. Therefore, the price in these countries, where it is banned, is no lower than the average in the rest of the world. One hypothesis that I venture to test, which falls beyond the scope of this paper, is that countries lack the tools to enforce a ban on the use of cryptocurrencies to the point of rendering them useless and, therefore, worthless. On the contrary, hostile but insufficient measures must have some effect, like that of the 'war on drugs':

[83] Juan Galt, "Is Bitcoin Headed for a Break in Fungibility?," Bitcoin Magazine, 22 December 2015.

> In addition, prohibition acts as a "tax" on sellers in the drug market. Would-be and current drug vendors must now incorporate fines, possible prison time, and the cost of evading capture into their business models. This tax drives higher-cost sellers (i.e., those unwilling or unable to incur these additional costs) out of the market.
>
> Such a change in the drug market does align with the goals of prohibition. If sellers are pushed out of the market, this limits the supply of drugs and raises prices. These higher prices, in turn, reduce the quantity of drugs demanded. However, these higher prices and the changes in the market structure caused by prohibition generate unintended consequences, ones that work against prohibition's stated goals.[84]

Bitcoin users are aware of the potential damage that state intervention can cause to the monetary system and how the introduction of Bitcoin into their domestic economy can undermine state control. It is worth quoting from one of the founding texts of the political movement that gave birth to Bitcoin:

> You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project.[85]

Regardless, and beyond the grandiloquent speeches, Bitcoiners are clear that only a joint government crackdown could put a stop to their cryptocurrency, as it is not difficult for individuals and companies to evade jurisdictions that take prohibitive measures in isolation.[86]

Gresham's Law: currency competition

Gresham's Law was recognized by several thinkers throughout history, although they are not worth mentioning in this paper; however, it entered the academic literature through the work of Giffen.[87] This law is succinctly formulated as 'bad money drives out good'. In greater detail, it

[84]Christopher J. Conye and Abigail R. Hall, "Four Decades and Counting. The Continued Failure of the War on Drugs," Policy Analysis No. 811, Cato Institute, 12 April 2017.

[85]Barlow, *A Declaration of the Independence of Cyberspace* (1996).

[86]Sebastian. Meunier, "Can Bitcoin Be Destroyed? 7 (Unlikely) Paths to Irrelevance," Coindesk, 29 January 2018.

[87]Robert Giffen, "The Gresham Law," *The Economic Journal* 1, no. 2 (1891): 304–06.

consists of the following: if we have a bimonetary economic system with a 'bad money' (which depreciates in value over time) and a 'good money' (which appreciates in value over time); then the bad money will tend to circulate more (since nobody wants to keep that currency and prefers to spend it) leaving the 'good money' (which the majority chooses to hoard) out of circulation.

This issue is particularly important for Bitcoiners, as they intend for Bitcoin to replace legal tender, and has been discussed since the beginning.[88] The question is to deduce which currency displaces fiat money, which will be legal tender, and which cryptocurrencies will operate in parallel.

If we consider that Bitcoin has intrinsic value and that its price tends to increase over time; and that legal tender currencies have no intrinsic value, and their price tends to decrease over time; we would conclude that Bitcoin is going to remain as a form of savings while legal tender remains in use for everyday consumption. However, certain factors make this scenario not precisely the one posed by Gresham's law. This law was conceived in a commodity-currency scenario, in which the minted currency was made of metals with intrinsic value. Competition arises between two coins with a nominal, legal value and another intrinsic value, given by the material from which they are made. Bad money is that whose nominal value exceeds its intrinsic value, and vice versa. In the case of Bitcoin as legal tender, we are dealing with a currency of pure nominal value versus one of pure intrinsic value (or, at least, without a legally sanctioned nominal value).

On the other hand, legal tender currencies are geographically limited in use (except for the U.S. dollar) while cryptocurrencies circulate worldwide. Einzig finds that a similar phenomenon occurs with what he calls 'primitive currencies':

> The operation of Gresham's Law in primitive communities is at times apt to be handicapped by the lack of adequate export facilities. The use of some primitive currencies is confined to a particular community and cannot be exported at all.[89]

In the case of legal tender, it is not transporting technology that imposes regional boundaries but national sovereignties. According to Gresham's Law, Bitcoin can be expected to gain ground internationally, while

[88] Noel. Jones, *Gresham's Law and Bitcoin, Bitcoin Theory*, accessed 17 June 2022.
[89] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 414.

within each country, it is relegated to a secondary status as a form of legal tender. In other words, Bitcoin faces Gresham's law at two distinct levels: local and global. At the regional level, it confronts the legal tender of each country. At the international level, it competes with the US dollar as a widely used and legal currency, on the one hand, and other cryptocurrencies, such as altcoins (which I will address in the next section), on the other.

Locally, Bitcoin is an impractical currency to use for everyday transactions, due to the high volatility of its price and payment confirmation times. In practice, the case of Argentina is a good example of its use as a form of savings, to the detriment of the peso, which is used as an instrument of expenditure, in strict compliance with Gresham's Law. As shown in Figure 24, during the period when the purchase of dollars was deregulated, bitcoin exchanges remained low. It was only in 2018, when economic policy began to falter, that they began to rise moderately. With the new exchange control, the rate increased more abruptly, and as the period of social isolation began during the COVID-19 pandemic, it rose even further, likely due to the physical limitations on accessing cash in the informal market.

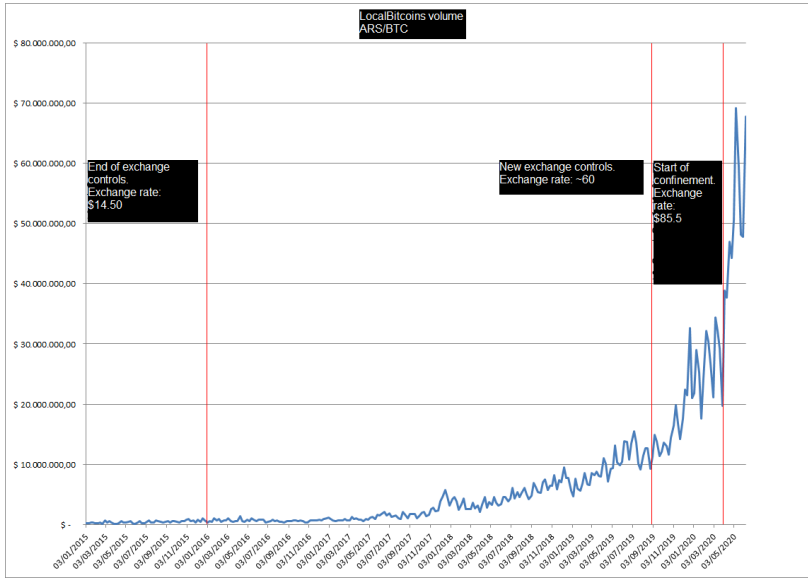


Figure 23: Volume of bitcoin trading transactions in Argentina during the period 2015-2020 with notes on government measures that affected the public's access to U.S. dollars. Sources: CoinDance, Ambito, BORA,[90] El País,[91] Perfil.[92]

At the global or international level, Bitcoin gained ground in international payments and remittance flows.[93] At the same level, but in another field, Gresham's law appears in Bitcoin's interaction with other cryptocurrencies. Being FOSS (Free and Open-Source Software), blockchain and cryptocurrency technology can be copied and modified without (legal) limits. That results in a massive proliferation of cryptocurrencies. Einzig says that:

> The total of primitive currencies in use is (…) not in contradistinction to the total of goods to be bought. The quantity of any one of these currencies is in contradistinction to the quantity of goods *plus* the quantity of the other currencies.[94]

CoinMarketCap, as its name suggests,[95] measures the market capitalizations of its more than 5,000 cryptocurrencies.[96] Among its principal metrics is Bitcoin's dominance, which is understood as the proportion of total market capitalization that corresponds to Bitcoin. This currently stands at around 65%.

> It seems justified to conclude that, unless there are fixed and effective parities between currencies that can be used indiscriminately, only the least valuable, or rather the most highly over-valued, amongst them fulfils effectively the part of money. The others largely assume the role of commodities with officially but ineffectively fixed prices. In that case the price level in the community concerned is apt to be determined not by the total volume of all currencies but by that of the one currency which functions effectively.[97]

Despite Bitcoin being the cryptocurrency with the largest capitalization, the currency with the highest traded volume is the Tether dollar, a cryptocurrency whose unit is equivalent to one US dollar. This is undoubtedly significant with respect to the use that Bitcoin adopts. Gresham's Law

[90] Presidencia de la Nación Argentina, "Aislamiento Social Preventivo y Obligatorio," Boletín Oficial de la República Argentina, effective 20 March, 2020.

[91] Alejandro Rebossio, "Argentina Libera el Control de Capitales," El País 17 December 2015.

[92] "Macri Vuelve al Cepo: Habrá que Pedir Autorización para Comprar Dólares," Perfil, 1 September 2019.

[93] Genny Díaz, "Apagones en Venezuela Revelan Uso de Bitcoin para Envío de Remesas en Latinoamérica," *Criptonoticias* (2019).

[94] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 422.

[95] Abbreviation for Coin Market Capitalization.

[96] Market capitalization is the product of the price of each unit by the number of existing units, in this case cryptocurrencies.

[97] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 424.

seems to cause Bitcoin to take on the character of a means of savings rather than a means of exchange. This will be developed further in the following subsection, on monetary functions.

Thiers' Law: currency substitution

A lesser-known law is the opposite and complementary of Gresham's Law, which the economist Peter Bernholz called "Thiers' Law," after Adolphe Thiers, a French politician who attested to the disappearance of the official currency during the French Revolution. This law holds instead that 'good money drives out the bad one.' How can this be? Is this a contentious subject on which economists have not yet reached a consensus? Not exactly. Even if it is the exact inverse of Gresham's law, Bernholz places Thiers' law at a later stage than Gresham's along a process of currency substitution:

> In period three, after official reserves have been exhausted, whereas the budget deficit remains, the government tries to maintain the parity (fixed exchange rate) between old and new money by making it legal tender and by trying to enforce its use with fines and penalties. As a consequence the bad money drives the good money out of the portfolios of the public. Gresham's Law works and the balance of payments is in deficit.
>
> In period four, after the good money has left the country and with an ongoing budget deficit still financed by money creation, even the severest penalties cannot maintain a fixed exchange rate. The price level and the exchange rate begin to rise at an increasing rate. The balance of payments turns into a surplus. Thiers' Law holds the good drives out the bad money. Finally, it should be mentioned that periods three and four are usually interwoven in reality, since the fines and penalties imposed by the government may not be sufficient to prevent an increase of the exchange rate, a premium or agio (that is the premium in per cent paid for the gold or silver money compared to the value of the paper money) of the good money in a black market.[98]

The consequences for Bitcoin are as follows: as long as legal tender or any other competing currency offers relative price stability, Bitcoin will remain relegated to a store of value function and driven out of circulation.

[98] P. Bernholz, Monetary Regimes and Inflation: History, Economic and Political Relationships (Edward wardElgar Publishing, 2003), 115.

As Bitcoin's price is expected to rise in the future, the reasonable thing to do is hoard it and spend the currency whose value is likely to diminish over time. However, if the competing currency's value is completely wiped out and nothing can be bought with it anymore, then Bitcoin would have to start circulating as a medium of exchange, effectively substituting for it.

◆ Properties

As I mentioned in a chapter of the first part, Jevons listed the properties of the material to serve as currency in order of priority, from highest to lowest. The matter is somewhat elusive when applying these principles to an immaterial object, but similar properties can be found that make the existence of digital currencies possible.

Utility and Value

> Since money has to be exchanged for valuable goods, it should itself possess value, and it must therefore have utility as the basis of value.[99]
>
> When once a substance is widely employed as money, it is conceivable that its utility will come to depend mainly upon the services which it thus confers upon the community.[100]

I have discussed the fundamentals of Bitcoin's value throughout the previous subsection. Here, it suffices to summarize that Bitcoin's value is given by its utility and scarcity. The mining work needed to produce more coins is variable and, therefore, does not serve as a standard. However, the intellectual work and development of the system do bring greater utility and value to the system.

[99] Jevons, *Money and the Mechanism of Exchange*, 32.
[100] Ibid., 33.

Portability

"The material of money must not only be valuable, but the value must be so related to the weight and bulk of the material."[101] Immaterial money has no physical weight or volume, but it does in computer terms. Moving cryptocurrencies from one territory to another, if done by the same owner, would not incur any costs, as he only needs to carry his private keys. However, transferring bitcoins to another person, regardless of their physical proximity, will incur a fee based on the value of the coins being transferred, not the weight or size of the transaction.[102]

To understand this, it is necessary to pause for a moment to consider how bitcoin transactions work. In the previous chapters, we saw that in each block, several new coins are produced. In terms of Bitcoin software, this is a new UTXO, a concept that has already been introduced and now requires further development. UTXO is an acronym for Unspent Transaction Output. If we follow the path of this output, it will be understood how it works. UTXO is like a check. Suppose that a miner mined 10 BTC; he will have an original UTXO of 10 BTC. If he wanted to move the 10 BTC in a single transaction, that UTXO would become an inflow of 10 BTC, and there would be an outflow of 10 BTC to another address. If, on the other hand, you wanted to send 1 BTC to another address and keep 9, you would still have to use the 10 BTC UTXO as an input, but you would have two outputs: one of 1 BTC to the destination address and another of 9 BTC to yourself. In this way, it is creating two new 'checks', two new UTXOs. Conversely, if an address has, for example, a 2 BTC UTXO and a 3 BTC UTXO, and wants to send 5 BTC to another, it will spend those two UTXOs of 2 and 3 BTC and create a new one of 5 BTC.[103]

The consequences for portability are as follows. In the first example, a transaction with one input and one output will be lighter than the second, with one input and two outputs. The more UTXOs used in a transaction, the heavier or larger it will be, since it consists of a larger amount of information. Since the fee to miners is measured in satoshis per byte, they

[101] Ibid., 34.

[102] Spanish speakers are used to talking about the weight of digital files ("this document weights 156 kilobytes"), whereas the English word for this is size, which is also used in Spanish, but less frequently.

[103] For further details on this, see Chapter 6, Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*.

pay more for transactions that occupy more space, as blocks have limited space to accommodate transactions.

This makes Bitcoin extremely useful for transferring large sums over long geographic distances, but inconvenient for small payments over short distances and in a short amount of time.

> The portability of money is an important quality not merely because it enables the owner to carry small sums in the pocket without trouble, but because large sums can be transferred from place to place, or from continent to continent, at little cost.[104]

All digital money complies to a significant extent with the portability criterion, but cryptocurrencies also provide autonomy with respect to possession. Until the creation of Bitcoin, digital money was always required to be in the hands of an institution (bank, payment service, etc.), known as a trusted third party, to be used in this manner. Blockchain technology allows, instead, true portability of digital assets.

Indestructibility

"If it is to be passed about in trade, and kept in reserve, money must not be subject- to easy deterioration or loss."[105] However, losses are commonplace and unrecoverable. The only way to spend bitcoins is with the proper private key, so coins hosted at addresses whose key no one possesses are lost. Coins can be lost in at least three ways: if a user forgets or loses the private key of addresses where coins were stored; if bitcoins are sent to an address for which no one owns the key; if a transaction is made with the OP_RETURN instruction in the script, rendering the output unspendable thereafter.[106]

On the other hand, complete system destructibility is dangerous, i.e., the entire network will cease to function. The chances of this happening are incredibly low because the system it relies on is distributed. For Bitcoin to cease functioning altogether, a complete disconnection of the Internet or a catastrophic global-scale phenomenon would be required.[107]

[104] Jevons, Money and the Mechanism of Exchange, 35.
[105] Ibid., 3 6.
[106] Bitcoin Wiki. "OP Return."
[107] Meunier, "Can Bitcoin Be Destroyed? 7 (Unlikely) Paths to Irrelevance."

Homogeneity and the Problem of Fungibility

The English word 'fungible' implies that the units of a given good are mutually interchangeable, i.e., every one of them is as good as any other.[108] Jevons on his part, Jevons speaks of homogeneity, not fungibility, and says, "All portions or specimens of the substance used as money should be homogeneous, that is, of the same quality, so that equal weights will have the same value."[109]

The fungibility of a currency is an indispensable property, which is why it is often taken for granted by most authors and in most of the examples discussed. However, in the context of cryptocurrencies, it is presented as a problematic aspect. The problem of homogeneity lies in the recording of transactions, which leaves open the possibility of tracing the history of any currency and differentiating it from others through network analysis. As soon as Bitcoin began to be used in Dark Net markets, various government agencies, law enforcement, and companies started investigating associated crimes. A pioneer company that tried to implement a method called 'coin tainting' was CoinValidation.[110] Concisely, what it set out to do was to blacklist addresses and mark the money passing through them: to make a chain of associations until it could be linked to a person's identity. This initiative unleashed a controversy in the forums about the problems that these processes would bring to the system:

> Some 'clean' coins would be easier to spend and transact with, while other 'less clean' or downright 'tainted' coins would be more difficult to use. Thus we would be left with a difficult-to-navigate and frustrating-to-use system whereby some coins are worth more than others (due to their varying spendability). And this largely defeats the purpose of a currency as a facile medium of exchange in the first place.[111]

[108]The original version contained made a reservation on this point, as there is an idiomatic problem when speaking about this, since the adjective 'fungible' in Spanish means that the object or good is consumed with use instead of mutually interchangeable.

[109]Jevons, Money and the Mechanism of Exchange, 37.

[110]Kashmir Hill, "Sanitizing Bitcoin: This Company Wants To Track 'Clean' Bitcoin Accounts," *Forbes* (2013).

[111]Goonsack, "What a Landmark Legal Case from Mid-1700s Scotland Tells us about the Fungibility and the Very Nature of Money– and Why we Should Care in light of the Recent CoinValidation Controversy," Reddit, (2013).

To mitigate this problem, coin mixers began to be used.[112] By mixing the coins, the chain of transactions corresponding to each one is confused, and thus they are 'cleaned' to some extent. A mixer can be a service where users pay to mix their coins, but this leaves them at the mercy of the service provider, who may be fraudulent and steal the funds, and also has access to information about the transactions they carry out. Other implementations have been taken directly to software, the most notorious being the ZeroLink framework.[113]

In any case, the problem of tainted currencies appears not to directly affect the value of some currencies against others, but rather the possibilities for trading. The measures taken by custodians, who intermediate the relationship between legal tender and cryptocurrencies, when they are accountable to certain official bodies, involve freezing the entire account associated with suspicious addresses rather than marking the coins themselves. On the other hand, only large companies can track money this way and flag addresses and coins; the average user is usually not concerned about the history of their coins and whether they are 'clean'. In addition, there is a large space of unregulated markets where they can be spent or sold without problems. Additionally, mixing services and software are popular enough for coins to be cleaned on a regular basis.[114]

Divisibility

> ...the material of money should be not merely capable of division, but the aggregate value of the mass after division should be almost exactly the same as before division.[115]

All digital money, being strictly numbers on computers, is plausible to be divided almost infinitely without losing a part in the process. However, payment services generally operate with units analogous to cash: two decimal places. Only in a few cases did they go as far as to add one or two more decimal places, without ever fully exploiting this capability. Bitcoin, on the other hand, is divisible to eight decimal places by default.

[112]"What are Bitcoin mixers?," *Bitcoin Magazine*.
[113]nopara73, "ZeroLink: The Bitcoin Fungibility Framework," (2017).
[114]Peter Chawaga, "As Analytics And Privacy Efforts Clash, Which Path Will Bitcoin Take?, *Bitcoin Magazine*. (2020).
[115]Jevons, *Money and the Mechanism of Exchange*, 38.

Table 9: Bitcoin units of measurement. Source: Bitcoin Wiki.

Unit	Abbrev.	Decimal (BTC)	Alternate names	Info
Algorithmic maximum		20,999,999.9769		Calculation
tam-bitcoin		2,814,749.76710656		1,0000,0000 tonal
mega-bitcoin	MBTC	1,000,000		Rare in context
kilo-bitcoin	kBTC	1,000		Rare in context
hecto-bitcoin	hBTC	100		Rare
Initial block subsidy		50		Until block 210000
bong-bitcoin	TBC	42.94967296		1,0000 tonal
Current block subsidy		12.5	block	As of block 420000
deca-bitcoin	daBTC	10		Rare
mill-bitcoin	TBC	2.68435456		1000 tonal
bitcoin	BTC	1	coin	SI base unit
san-bitcoin	TBC	0.16777216		100 tonal
deci-bitcoin	dBTC	0.1		Rare
ton-bitcoin	TBC	0.01048576		10 tonal
centi-bitcoin	cBTC	0.01	bitcent	Frequent until 2013 bubble
milli-bitcoin	mBTC	0.001	millibit, millie	Occasional
bitcoin	TBC	0.00065536		Tonal base unit
bitcoin-ton	TBC	0.00004096		0.1 tonal
bitcoin-san	TBC	0.00000256		0.01 tonal
micro-bitcoin	BTC	0.000001	bit	Frequent
bitcoin-mill	TBC	0.00000016		0.001 tonal
		0.0000001	finney	
bitcoin-bong	TBC	0.00000001		0.0001 tonal
	sat	0.00000001	Satoshi	Blockchain value
	msat	0.00000000001	millisatoshi	Payment channel value

The minimum value that the Bitcoin network accepts is one satoshi, equivalent to one hundred millionth of a bitcoin, which is used, among other things, to measure transaction fees. However, divisibility does not stop there, as second-layer protocols such as Lightning payment channels accept units up to a thousand times smaller, and tools can be developed to divide the units further if necessary.

On the other hand, such divisibility, when it goes hand in hand with a very large increase in the value of the units, as in the case of Bitcoin, generates an adverse psychological effect: when operating with very small numbers such as 0.002, 0.0007, etc., one has the feeling that one is not moving large values; in contrast, $3200 or $1120 seem more important numbers; but in the conversion of BTC (Bitcoin) to ARS (Argentinean Peso) they are equivalent amounts as of today (August 2020). Similarly, this problem arose in the introduction of coins with a nominal value in communities that exchanged products by weight or size:

> ...since time immemorial many primitive races had been accustomed to bartering goods of approximately equal importance against each other, which meant equal weight or size. They could not easily grow

> used to the strange idea of giving bulky goods in return for small coins.[116]

Stability of value

> It is evidently desirable that the currency should not be subject to fluctuations of value.[117]

If there is one property that Bitcoin clearly does not fulfil, it is this. Bitcoin's exchange value is highly unstable, which is one of the main arguments used by its detractors to argue that it is not a valid monetary instrument.[118] Bitcoin's volatility is a widely studied, measured, debated, and unresolved issue.

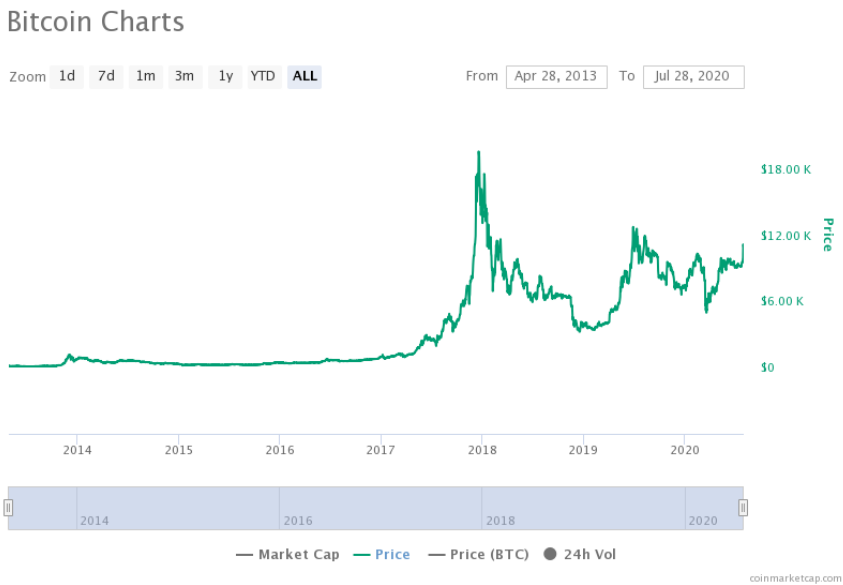


Figure 24: Historical bitcoin price on a linear scale. Source: CoiuMarketCap.

[116] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 507.
[117] Jevons, *Money and the Mechanism of Exchange*, 38.
[118] Karl Denninger, "BitCon: Don't," Mark. Tick. ® - *Commentary on the Capital Markets*, (2013).

Figure 25: Historical bitcoin price on a logarithmic scale. Source: CoinMarketCap.

The price variation on a linear scale (Figure 25) may give the impression that the price remained constant for the first eight years and then began to vary abruptly in 2017. However, that entire period from 2013 to 2017 is marked by difficulties that were rendered insignificant as price variations increased by orders of magnitude. The logarithmic scale (Figure 26), on the other hand, shows the evolution of the same value in these various orders of magnitude, and it can be seen how this apparent stability breaks down into oscillations between USD 100 and USD 1000, and from 2017 onwards, oscillations between USD 5000 and USD 10000.

Finally, Figure 27 illustrates the evolution of the same volatility, measured in standard deviations of daily returns, over a slightly longer time scale (2011-2020). Volatility itself is volatile, as it oscillates abruptly between 5 and 15 for the first four years and then declines. The volatility trend appears to be regressive over the years, and some scholars estimate that it will decrease as the Bitcoin market grows.[119] Certain financial instruments can reduce the volatility of an asset, such as futures and deriva-

[119]Radoslav Albrecht, "Bitcoin Volatility – The 4 Perspectives," Bitcoin Magazine, (2013).

tives markets, whose development runs parallel to the growth of the primary Bitcoin market.

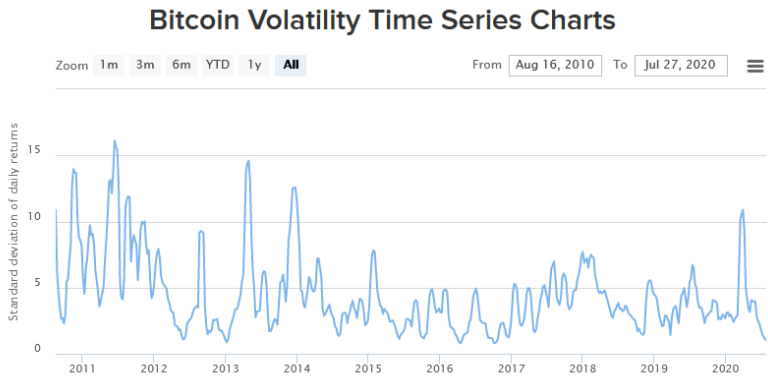


Figure 26: Historical bitcoin volatility. Source: BuyBitcoinWorldwide.com.

Cognoscibility

> By this name we may denote the capability of a substance for being easily recognized and distinguished from all other substances. As a medium of exchange, money has to be continually handed about, and it will occasion great trouble if every person receiving currency has to scrutinize, weigh, and test it. (...) Hence the medium of exchange should have certain distinct marks which nobody can mistake.[120]

This quality in Bitcoin is indisputably fulfilled in contrast to the previous one. The blockchain system was developed with the purpose of avoiding double spending and fraud. If a transaction contains an output greater than the sum of its inputs or if it attempts to spend a previously spent input, it is considered invalid by the system. Bypassing security and reversing a transaction or creating new units requires more computational effort than half of the miners combined, ensuring the system's security. An individual can be cheated out of bitcoins from the test network or invalid transactions, but the system itself has not been breached since its early testing phases, when it was still incomplete.

[120] Jevons, Money and the Mechanism of Exchange, 40.

◆ Functions

This section examines Bitcoin in light of the distinct functions assigned to it by economic theory. It aims to determine to what extent it fulfills these functions or whether it does so successfully, since its quality as a monetary instrument depends on this.

Einzig, theorizing on the functions of currency, establishes, albeit not systematically, a particular hierarchy of trust that a monetary instrument requires to fulfil specific functions.[121] The usefulness of such a hierarchy is doubtful, since in many cases in his own studies, and with Bitcoin, as will be seen, a higher hierarchy function is fulfilled without fulfilling a lower one. However, I thought it prudent to synthesize such a hierarchy into the following Table.

Table .1: Einzig's hierarchy of trust and monetary functions.[122]

Trust Degree	**Function**	**Function**
4	Storage of value	Means of deferred payments
3	Standard of value	Standard of deferred payment
2	Means of exchange	Liquidity reserve
1	Means of non-commercial of payment	

Means of Exchange

This is the most important function that the Bitcoin community intends Bitcoin to fulfil. This is not surprising given that Mises's theory, the most widely accepted, regards it as unique and fundamental. If it is not a medium of exchange, it is not a currency, according to this author. It is this function that is commonly referred to when talking about Bitcoin's 'adoption'. This chapter is, therefore, closely related to the Extension of use and restrictions in the previous subsection concerning the value of Bitcoin.

> A MEDIUM of exchange is an object conforming to certain standards of uniformity that is widely accepted in payment for goods

[121] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 439, 442, 448.

[122] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects.*

> and services, because the recipient can easily use it for making similar payments.[123]

This concise definition encapsulates what a medium of exchange is, and all the problems that arise when trying to introduce a new medium of exchange into everyday practice can be derived from it. The most important of these is the bootstrap problem, also known as the chicken and egg problem: for merchants to accept Bitcoin as payment there must be many people willing to pay with it, but for a consumer to want to pay with Bitcoin there must be many merchants who already accept it, so who is going to take the first step; or, in other words, each individual subject prefers to use the medium of exchange that everyone else uses because they have greater liquidity; and nobody is going to want to use a medium of exchange that nobody else uses. In the section on social currencies, we can see how a community develops its own monetary instrument; on the other hand, legal tender has the state's coercive power to force its use as a medium of exchange. Bitcoin does not have either of these two supports, or at least it has a community, but not of the same type as the social currencies referred to previously. In the chapter on the origin of Bitcoin, I elaborated on this issue and the initial kick-off of the Bitcoin Pizza Day. I will now explain how Bitcoin continued to serve as a medium of exchange.

Following the initial pizza push, small sales started to be made on the BitcoinTalk forum and were subsequently accepted on Dark Web black markets.[124] By 2013, there was speculation about what the subsequent evolution might be. Jon Matonis, a Bitcoin developer, authored an article in Forbes magazine in which he posited that the cryptocurrency is the System D of currencies.[125] He predicted that it would find its largest user base in those economic actors outside the formal system, individuals who have little confidence in the currency they usually use, who are excluded from the financial system, and/or who have the technical capacity to access it.

But eight years later, can it be proven that this has happened? Coinmap, a website that locates Bitcoin-accepting businesses worldwide, shows the highest density of Bitcoin-accepting businesses in North America, Europe, and Southeast Asia.

[123] Ibid., 431.

[124] Noel Jones, "Bitcoin, Bootstrapping, and the Black Market," Bitcoin Theory, (2013).

[125] Jon Matonis, "Could Bitcoin Become the Currency of System D?," Forbes, (2012).

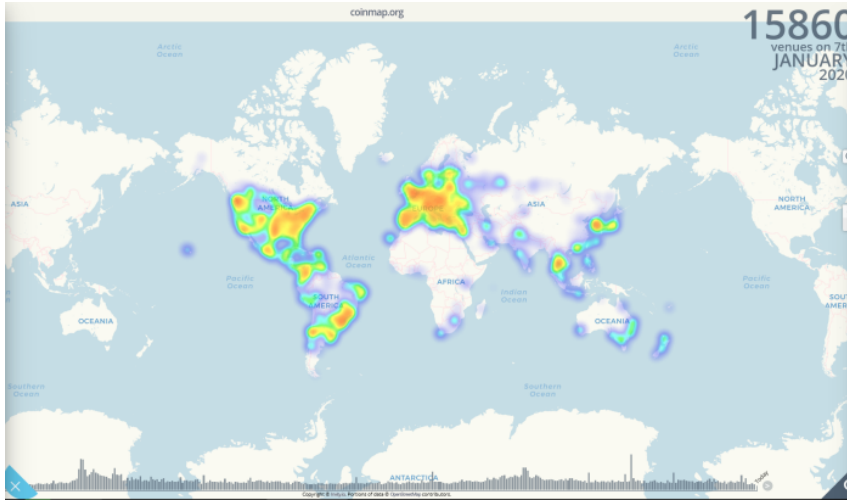


Figure 27. World map with density of merchants accepting Bitcoin or other cryptocurrencies. Source: http://www.coinmap.org/view/.

These are not what we might call marginal areas. On the contrary, they are areas where formal economic activity is concentrated. So, what happened? In principle, governments did not unanimously ban cryptocurrencies, relegating them to underground trade, as Matonis assumed. As I explained in the chapter "Supply, Demand, Quality, and Quantity," the primary source of information regarding prices and trading volumes of cryptocurrencies comes from the financial sector, rather than the so-called real economy. This financial sector is not just a System D, a copy of the legal stock exchanges made for cryptocurrencies, entirely outside of legality. Although it initially started that way, the cryptocurrency financial sector was gradually incorporated into the government-regulated financial sector worldwide. So much so that today, major cryptocurrency exchanges require their users to fill out forms to comply with regulations known as KYC (Know Your Customer) and AML (Anti-Money Laundering);[126] moreover, traditional financial services have been incorporating cryptocurrencies into their operations, such as futures exchanges.[127] Even banks are starting to operate in this space.[128] Other services, such as ETFs (Exchange Traded

[126]Of course, this being so contrary to cypherpunk idiosyncrasy, there are several markets that do not comply with such regulations and even guides and listings of such markets. For example, https://kycnot.me/.

[127]CME Group, "Bitcoin Futures and Options."

[128]Nathan DiCamillo, "This Liechtenstein Bank Can Now Custody Crypto," (2020).

Funds) have not been successful but are still trying.[129] I will elaborate on the implications of this in the Foreign Exchange chapter below.

Regarding the real economy, the exchange of goods and services is related to what was developed in the chapter on Gresham's Law. As I have already discussed in that chapter, Bitcoin is preferred for storing value rather than as a medium of exchange. However, this is not to say it will never perform as the latter. Additionally, in the chapter 'Extension of Use and Restrictions,' I mentioned the commercial use of Bitcoin and the challenges of obtaining reliable macroeconomic data.

However, it is possible to analyze the microeconomic levels and learn about certain small-scale trading practices that utilize bitcoins as a medium of exchange. As I mentioned, the first markets to utilize it were BitcoinTalk forum enthusiasts, starting in 2011, and the underground economies of the Dark Web, with Silk Road (2011-2013) serving as a landmark.[130] In 2014, the online sales company Overstock began accepting bitcoins as a means of payment, and Bitrefill, a company that brokers the purchase of various products from online merchants using cryptocurrencies, began operating. Additionally, the Dark Market hackathon was organized, which in 2016 would become Open Bazaar, a marketplace structured directly with P2P technology, in which one pays exclusively with cryptocurrencies.

In terms of face-to-face trading, progress was certainly slower, but it has been made nonetheless. Coinmap's historical information is helpful in this respect.

[129]Nikhilesh De, Stan Higgins, and Muyao Shen, "SEC Rejects 9 Bitcoin ETF Proposals," Coindesk (2018).

[130]Wikimedia Foundation, "Silk Road (marketplace)."

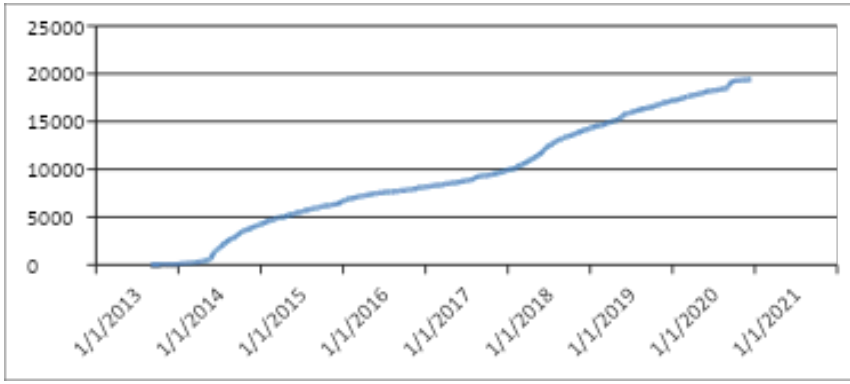


Figure 28: Number of shops listed on CoinMap over time. Source: own elaboration based on the data published in https://coinmap.org/api/v1/venues/.

As seen in Figure 29, from 2014 onwards, small retailers accepting Bitcoin increased in number and continued to do so steadily. There is, however, one problem with this data: there is no definitive closing date for a business. As a result, the number is overstated, including businesses that are no longer in operation, or understated because they have been removed. The record that they ever existed is gone. I am inclined to think that the former is more often the case. On the other hand, this also does not tell us much about the volume of bitcoin transactions that these shops have, which is, according to my research, low or non-existent:

> We would like to see more [customers paying with bitcoins], but there are not many. Those who tend to use them are those who are just starting to learn about them. Those who already know about them prefer to keep them.[131]

Accessibility does not seem to be a problem for the traders, according to another testimony I collected:

> ...It is not too complicated to learn how to use it and it does not need too much. Of course you have to have a computer or a mobile phone, but you don't need a lot of knowledge. It is just a matter of researching.[132]

[131] From an unpublished interview between the author and the owner of Il Ponto Mercato restaurant, located in the city of Buenos Aires, (2018).
[132] Ibid.

Another trader was even clearer about the difference in functions and described Bitcoin as better for storing value than as a medium of exchange:

Figure 29: Venezuelan street vendor accepts three cryptocurrencies. Could not corroborate the source.

> **G:** -...Bitcoin is not the currency that I would like to use for... I mean, it is more like a savings, no. It is like comparing gold with bronze or with banknotes... I mean, Bitcoin is like gold, and I need something like a banknote that I can make quick transactions with, that I do not have to wait: "well, they have already confirmed three of... I do not know how many."
>
> **L:** -So, uh. Because yesterday they told me they had Ethereum as the most important one.
>
> **G:** -Yes
>
> **L:** -It is because it is done faster
>
> **G:** -Yes, and because, as I told you, we have the platform that converts directly into pesos. We have the speed of transactions... for me it is more convenient. Of course, obviously you can keep them, you can exchange them to Bitcoin, it is a very versatile market. But yes, primarily ETH. Besides, that is what I mined the most.[133]

[133]From an unpublished interview between the author and the owner of Burgertify restaurant, located in the city of Buenos Aires, (2018).

Figure 30: Advertisement from a shop in Buenos Aires. Source: Instagram

A key point that helps adoption as a medium of exchange is that opening such a payment channel is not costly for a business. Unlike centralized systems, such as credit card payment systems, a cryptocurrency wallet is free of charge and has no maintenance costs. In addition, fees are not calculated as a percentage of the amount transferred, so they are typically 1% or less. Special equipment is not even required, as these are software implementations only. Hybrid payment services were developed anyway, including XPOS from Pundi X and credit/debit cards that accept Bitcoin funds.[134] Simply downloading and installing a computer or mobile phone program, or registering with one of these online "banks," is enough to start accepting these currencies. This means that even if customers do not use this money very often, they can keep that channel open in case they eventually do. This, in turn, allows inexperienced users of this money to have more opportunities to try it out in real economic transactions.

> If it does not exceed the credit card percentage, it is fine. The credit card is 3%, if it does not exceed that then great. I do not think it does, I think the most they have charged is 1.5% for the SatoshiTango bank transfer.[135]

Which brings us to one of the points where Matonis's informal economy hypothesis was wrong. He believes that people in the informal sector will use them to access specific financial tools they currently lack, but liquidity is the primary problem a precarious worker faces. He will only accept money that he can spend immediately, as Ravenna discovered in his exper-

[134]John Ladeluca, "Best Bitcoin Bitcoin Debit and Credit Cards in 2020 - InsideBitcoins," InsideBitcoins.com (2020).

[135]From an unpublished interview between the author and the owner of Burgertify restaurant, located in the city of Buenos Aires, (2018).

iment in the Barrio 31 of Buenos Aires.[136] That is why, I understand, the merchants who have turned to accepting bitcoins the most are businesses with a certain amount of capital, who could afford a second means of payment. They also work with financial services that allow them to liquidate these digital assets more quickly.

The cases where widespread daily use of Bitcoin has been recorded are extreme, such as Palestine and Venezuela.[137] In the latter case, only moderately, as it was mainly miners who, taking advantage of subsidized energy, produced cryptocurrency domestically to procure subsistence goods by spending them in online shops. Recently, there have been reports of street artisans beginning to accept them. For its part, the Venezuelan government has oscillated between hostility towards cryptocurrencies, particularly the miners who utilize state-subsidized energy to produce them,[138] and promoting their acceptance, while also creating its own national cryptocurrency to circumvent international embargoes. Other governments, such as Bolivia, mentioned above, and, more recently, Russia, have banned Bitcoin transactions outright.[139] While it is unlikely that they will succeed in eradicating all Bitcoin transactions, such policies shift the entire economy to the informal sector. It is an open task to investigate whether Matonis's prognosis is being realized in these countries.

Measure of value or unit of account

> STANDARD of value is a common denominator or unit of account in terms of which the prices of goods and services are regularly measured and expressed. (…) Prices are figures expressing the numbers of these units representing the equivalents of various goods or services. (…) unless there is a separate standard of value that is different from the medium of exchange, the use of the latter implies the use of the former. (…) A standard of value is a unit in which prices are apt to be quoted also independently of any actual exchange transaction.

[136] Florencia Ravenna, *What the Residents of Barrio 31 Slum Taught us About Bitcoin*, (2019).

[137] Palestine: Leigh Cuen, "In Palestine, Civilians Are Using Bitcoin More Than Hamas," Coindesk, (2019). Venezuela: Iván Gómez, "Bitcoin Contra el Autoritarismo: Caso Venezuela." Criptonoticias, (2020).

[138] Esparragoza, "Mineros Venezolanos Apagan sus Equipos por Temor a Persecución Policial."

[139] José Colmenares, "Putin Firmó ley que Prohibe Pagos con Bitcoin y Criptomonedas en Rusia." CriptoNoticias - Bitcoin, Blockchains y Criptomonedas, (2020).

Rank	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$173,053,001,906	$9,400.78	$17,899,756,478	18,408,362 BTC	-0.48%	
2	Ethereum	$25,738,493,825	$231.03	$6,721,396,645	111,405,246 ETH	-0.82%	
3	Tether	$9,216,594,265	$1.00	$21,297,293,903	9,187,991,663 USDT *	0.14%	
4	XRP	$8,462,536,300	$0.191210	$1,050,021,767	44,257,803,618 XRP *	-1.06%	
5	Bitcoin Cash	$4,364,720,439	$236.71	$1,307,785,442	18,438,750 BCH	-1.36%	
6	Bitcoin SV	$3,225,435,866	$174.94	$900,740,532	18,437,340 BSV	-1.49%	
7	Litecoin	$2,824,507,965	$43.47	$1,590,976,447	64,981,476 LTC	-1.09%	
8	Binance Coin	$2,508,083,319	$16.13	$178,114,561	155,536,713 BNB *	-1.45%	
9	EOS	$2,360,356,569	$2.53	$1,181,304,716	933,603,596 EOS *	-1.17%	
10	Cardano	$2,114,115,775	$0.081541	$251,005,262	25,927,070,538 ADA	-1.05%	
11	Crypto.com Coin	$2,003,402,590	$0.114900	$44,679,536	17,436,073,059 CRO *	-0.39%	
12	Tezos	$1,978,187,360	$2.70	$137,224,306	733,364,642 XTZ *	1.68%	
13	Chainlink	$1,462,419,107	$4.18	$302,624,006	350,000,000 LINK *	0.51%	
14	Stellar	$1,442,248,022	$0.070900	$404,004,122	20,342,066,057 XLM *	-1.14%	

Figure 31: Cryptocurrency prices. The graph on the right shows the evolution of the price in dollars over the last 7 days. A similar trend can be observed for all but number 3, as its price is adjusted to the US dollar. Source: CoinMarketCap

> (…) if an object serves as a standard of value it must be valuable, but it need not have intrinsic value [to be a standard of value]. (…) A standard of value need not, however, be even a fiduciary currency. It need not necessarily be a medium of exchange at all. It may be a purely fictitious unit which has no concrete existence and has therefore no value whatsoever.[140]

Bitcoin does not function as a measure or standard of value because its price fluctuates significantly over a brief period. The measure of value for all cryptocurrencies is the US dollar. Some enthusiasts reject the dollar standard with the tautology '1 BTC = 1 BTC', arguing that Bitcoin is, or should be, its own standard and fulfill the function of a measure of value. In reality, Bitcoin partially fulfills this function compared to other cryptocurrencies, as relatively few are traded directly in dollars, and most are exchanged for Bitcoin. Therefore, the prices of these cryptocurrencies are converted into dollars by first being converted into bitcoins. This means

[140] Paul Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 436-437.

that when the price of Bitcoin changes abruptly, the others follow the same trend, as shown in Figure 32.

> For a unit to qualify for being adopted as a standard of value it must enjoy a higher degree of confidence than that required for being able to fulfil the function of the medium of exchange.[141]

This may indicate that Bitcoin still lacks much trust, as it has not yet fulfilled the first of these two functions.

Finally, Einzig points out that:

> In many instances when modern money found its way into primitive communities, for a long time it was used within the community as a standard of value to a much greater extent than as a medium of exchange or a store of value or a standard of deferred payment.[142]

Bitcoin would be, in any case, making a reverse journey, as a 'primitive' money incorporating itself into a 'modern' economy, fulfilling those last functions initially. I will elaborate further on this issue in the following section.

Store of Value

Already briefly referred to in previous chapters, this is the function most frequently reported by the press and Bitcoin enthusiasts, because it is the one it has performed best so far. "A STORE of value is an object in which wealth is held exclusively, or at any rate primarily, for the purpose of preserving the value it represents."[143] In the case of Bitcoin, it is not only stored to maintain wealth, but also to increase it in the long term. This confuses individuals who consider buying bitcoins as *an investment* in them, which is not the same thing. Bitcoins per se are not productive capital.

Einzig points to a controversy within economic science about this function and the monetary instrument quality of the good that possesses it:

> Most economists consider store of value as one of the essential functions of money. A dissenting opinion is voiced, however; that of Walker who maintains that "when a commodity comes to serve as a

[141] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 439.
[142] Ibid., 440.
[143] Ibid.

> store of value it ceases to be money". (…) On the other hand, Helfferich holds the view that money is eminently suitable for store of value, because it gives the greatest freedom of action for unforeseen events.[144]

Against this, he concludes, "In order that an object serving as a store of value should be regarded as money, it must be able to perform at least one other monetary function." Therefore, it is not enough for Bitcoin to store value to enter the world of currencies in good standing. It must somehow defend at least one of the other functions, or it could become a kind of intangible luxury good. Analogous to jewelry and high-end cars rather than hard cash. However, even if it were to lose these other functions, its value would not necessarily be negatively affected, since

> When primitive money is replaced by modern money, the former is apt to retain its rule as a store of value long after it had ceased to perform its other monetary functions. (…) The limitation of the functions of primitive money does not necessarily cause a decline in its value. On the contrary, there are instances in which it actually appreciated in terms of modern money and of goods.[145]
>
> An object serving as a store of value need not necessarily have full intrinsic value. Confidence in fiduciary currencies must be very strongly established, however, in order that they may be considered suitable as a store of value. In this respect there is material difference between store of value and medium of exchange. The former requires a much higher degree of confidence. From this point of view, its qualifications are identical with those of a standard of deferred payments.[146]

In this sense, Bitcoin can be considered to have achieved an elevated level of trust, fulfilling the function that requires the most trust.

Finally, Einzig discusses the advantages and disadvantages of stores of value, with the latter being more significant than the former.[147] The main benefit is that holding a store of value means that a liquidity reserve (the next chapter's subject) is available if needed. Another advantage is that

[144] Ibid., 441.

[145] Einzig, Primitive Money in its Ethnological, Historical and Economic Aspects, 443-444.

[146] Ibid., 442.

[147] Fortunately for Bitcoin, many of these disadvantages have to do with the nature of the goods used for storage, such as livestock, which in large numbers ruin grazing land; or weapons or slaves, the accumulation of which comes with warfare.

an asset that serves as a store of value can, in turn, be used as capital (as is the case with cryptocurrencies). In recent years, what is known as DeFi (Decentralized Finances) has been developing, in which cryptocurrencies can function as capital. I will deal with this topic in a later chapter.

On the downside, we find that storage takes goods with practical utility or capital out of circulation. In the case of cryptocurrencies, the former is not a significant problem given their enormous divisibility, which creates a virtual impossibility of a lack of circulating cash for transactions. Nor does it represent a problem because its practical use is limited to serving as a monetary instrument, unlike other types of goods that have multiple uses. At the level of capital investment, there can be a contradiction between hoarding to safeguard value, but leaving a large amount of dead capital; or spending and investing to expand the possibilities of trade, but risking losing that fortune or the future fortune into which that saving could be converted, as every Bitcoin Pizza Day reminds us.

Liquidity Reserve

Keynes first introduced the concept of liquidity in his 1930 *Treatise on Money,*[148] referring to the ease with which an asset can be exchanged for goods, akin to Menger's notion of 'marketability'. The liquidity reserve function is thus closely related to a store of value and a medium of exchange, since the medium of exchange is the most liquid asset. However,

> An object may be qualified to serve as a liquid reserve without necessarily being used as a medium of exchange in a community where non-commercial payments are of considerable importance. (...) Since they are at the same time a standard of value and a store of value they undoubtedly play an important monetary part in the economy of the community. (…) Nor is the function of money as a liquid reserve necessarily identical with that of the store of value. (…) Liquid reserves are intended for possible use in the relatively near future and need not necessarily assume the form in which they are safeguarded against long-run depreciation.[149]

[148] John Maynard Keynes, "A Treatise on Money: The Pure Theory of Money," In *The Collected Writings of John Maynard Keynes*, Vol. 5 (2012); and "A Treatise on Money: The Pure Theory of Money," In *The Collected Writings of John Maynard Keynes*, Vol. 6 (2012).

[149] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 444.

On this point, Keynes is even more emphatic:

> … it is a recognized characteristic of money as a store of wealth that it is barren; whereas practically every other form of storing wealth yields some interest or profit.[150]

According to him, a subject will prefer to hold cash for four reasons, which he referred to as liquidity preferences: consumer spending, business, precaution, and speculation. However, Keynes does not stop to define what liquidity is or what an asset needs to become liquid. He already takes it for granted that money, in its chartal form, is the most liquid asset.

Einzig, on the other hand, does:

> In order to fulfil the requirements of liquidity, a primitive money must assume a form that is freely acceptable for all payments, large or small, that are customers in the community. Any money whose use is confined to certain types of payments is only qualified for serving as a liquid reserve to a limited extent (…). The fact that as a result of the "multi-centric" character of the monetary system, the monetary supply accumulated as a liquid reserve or as a store of value cannot be used indiscriminately in every sphere does not necessarily disqualify primitive currencies from serving as liquid reserves.[151]

Bitcoin would therefore be in an intermediate situation: although it is the most liquid asset in the crypto economy, which was formed around it, in the broader economic sphere, where it competes with legal tender, it is an illiquid asset because it is not widely accepted.

Means of Non-commercial Payments

Einzig greatly emphasizes the non-commercial use of many coins, which he refers to as primitive. This use can be of various kinds: payment of tribute or taxes to a political authority, marriage dowries, ornamental, ceremonial, religious, blood money (money paid to the family of a murdered person as compensation), and ransom in cases of kidnapping.

Bitcoin appears to be concerned only with the first and last of these, both in a very special or limited manner. The first, taxation, is of interest only when taxes are paid in Bitcoin, not where profits are taxed

[150] John Maynard Keynes, "The General Theory of Employment," Quarterly Journal of Economics 51, no. 2 (1937), 215–16.

[151] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 445.

in cryptocurrencies. Most jurisdictions already have some form of legislation regulating the business of cryptocurrencies within their territory, i.e., the companies that deal with them and their customers located in that jurisdiction, since cryptocurrencies are de-territorialized objects.

Most jurisdictions, I said, already provide for some form of cryptocurrency trading and impose taxation on the profits made from cryptocurrencies by individuals, whether legal or natural. The number of jurisdictions that directly tax cryptocurrencies, Bitcoin at least, is much smaller, but not non-existent. In 2017, some Swiss cities started allowing citizens to pay taxes directly in Bitcoin.[152] In late 2018, the state of Ohio began doing so, the first jurisdiction in the United States.[153] Shortly thereafter, a Canadian city imitated those Swiss cities.[154] There does not appear to have been a widespread trend of this, as there was in taxing cryptocurrency traders and investors and in efforts to prevent money laundering and terrorist financing. This could be because the taxation of bitcoin is a strategy aimed at attracting certain technology companies to the jurisdiction, an interest limited to a select few. At the same time, most states are interested in aligning the cryptocurrency market with their existing regulations.

Regarding the second of the aforementioned non-monetary uses, and on the opposite side of the law, there is what has come to be known as ransomware. This word, a combination of "ransom" and "software," refers to a computer program that carries out a hijacking. Not a kidnapping of people, but of information. This type of program infiltrates as a virus or Trojan horse, without the user's knowledge, and attacks by encrypting files that are preferably valuable to their owner, rendering them unusable. It then offers the key to restoring them in exchange for a bitcoin ransom. Such attacks gained popularity along side Bitcoin, with their milestone being the worldwide WannaCry attack, which affected more than 200,000 computers in 150 countries.[155] After that massive attack, the popularity of ransomware increased year after year and is listed among the computer security trends of the last few years.[156] However, Bitcoin is not the only

[152]David Meyer, "This Place Lets You Pay Your Taxes In Bitcoin," *Fortune* (2017).
[153]Paul Vigna, "Pay Taxes With Bitcoin? Ohio Says Sure," *Wall Street Journal* (2018).
[154]*Bitcoin Magazine*, (2019).
[155]Wikimedia Foundation, "WannaCry Ransomware Attack."
[156]Kim Porter, "Cyberthreat Trends: 15 Cybersecurity Threats for 2020," NortonLIfeLock, (2020).

alternative to carry out these payments, nor is it the most suitable, given the limitations of its anonymity. As evidenced by the attack on Telecom in July 2020,[157] the so-called privacy coins, which I will discuss in a later chapter, could be the preferred ones to use in these attacks.

Now, in economic terms, this trend has several effects on Bitcoin. The most immediate impact is that it increases the demand for bitcoins by forcing large payments to be made via bitcoins. A less direct impact is that it functions as a form of propaganda by forcing certain individuals to use the system without prior knowledge. When the non-specialized press publishes news about these attacks, a wider audience, including niche technology enthusiasts, learns about the event. Such publicity, however, is not necessarily positive. Many people who are only familiar with Bitcoin or cryptocurrencies through news stories about their use by criminals are more likely to develop an aversion to them than an interest, which can discourage the growth of their user base.

Medium and/or standard of deferred payments

> STANDARD of deferred payments is a monetary unit in which liabilities maturing at some future date are expressed.[158]
>
> In order that an object in whose terms deferred payments are fixed should qualify for the role of standard of deferred payments even if it does not perform any other monetary functions, it is necessary that it should be used systematically as a standard of deferred payments to be made by people not engaged in the production of the objects in question.[159]

These functions are perhaps the most challenging to address and even more difficult to implement in relation to Bitcoin, as they pertain to the ideas guiding its development. One of Bitcoin's main objectives is to supplant debt-based monetary instruments and national currencies, or at least to offer an alternative. In practice, this translates into its deflationary tendency,[160] which, unlike inflation, discourages long-term lending.

[157]"Telecom: Un Ataque de Ransomware Afectó a sus Servicios; le Pidieron US$7,5 Millones de Rescate." La Nación, (2020).

[158]Einzig, Primitive Money in its Ethnological, Historical and Economic Aspects, 446.

[159]Ibid., 447.

[160]The reasons for this trend will be explained in the following section, on Bitcoin monetary policy.

Deflation, for monetarists[161] and Keynesians, i.e.,[162] the two dominant schools of the discipline, is associated with economic recession, as explained in the debt-deflation theory,[163] and therefore advocates inflationary and debt-based monetary systems.[164]

Bitcoin's philosophy is radically different. As I explained in the chapters on value, as the utility of the payment system increases and the supply of new monetary units runs out, the latter's value will increase. So, interest-bearing loans would be excessively difficult to repay if they were fixed in bitcoins. In Einzig's terms:

> From the point of view of the standard of deferred payment, as from that of the store of value, the confidence factor is of great importance. Since such payments are apt to cover a more or less long period, stability of a standard of deferred payments, in order to be suitable, has to command a higher degree of confidence than a medium of exchange, a means of unilateral payment, or a standard of value for current transactions.[165]

As I explained in the relevant chapter, Bitcoin is not a reliable measure of value, at least not currently, due to its highly unstable price. Without being a standard of value for immediate transactions, it is understandably even more unviable to measure the value of deferred payments.

> Every standard of value, though good enough to serve the requirements of current transactions, may not command sufficient confidence to be acceptable for a standard of deferred payments which imply confidence in the stability in the long run. Every standard of deferred payments, on the other hand, should qualify from the point of view of confidence to serve as a standard of value, although it is conceivable that the value of an object might fluctuate erratically from day to day but might remain basically stable over a long period.[166]

Once again, this is not the case.

[161] M. Friedman and A.J. Schwartz, "Money and Business Cycles." Review of Economics and Statistics 45, no.1 (1963), 32.

[162] J.M. Keynes, *The General Theory of Employment, Interest and Money*, 244.

[163] Irving Fisher, "The Debt-Deflation Theory of Great Depressions," *Econometrica* 1, no. 4 (1933), 337–57.

[164] David Graeber, *Debt: The First 5000 Years*, (Melville House Publishing, 2012).

[165] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 448.

[166] Ibid.

> …primitive money serves not only as a unit of account in terms of which deferred financial obligations can be expressed, but it fulfils also the function of providing the actual means in which such payments are contracted and discharged. (…) Through the combination of these two functions it forms the basis of credit systems in communities which have advanced beyond the stage of payments in kind but which have not yet reached the stage of payment in coins.[167]

Without fulfilling the function of a standard or measure of value for deferred payments, it experiments with giving and cancelling loans in bitcoins and financializing the crypto economy, in DeFi, which I will elaborate on in the chapter on smart contracts. In addition, the Bitcoin script contains the OP_CHECKLOCKTIMEVERIFY function (number),[168] which means that an input cannot be spent until a particular point in time, providing a native facility for deferred payments that has not yet been fully exploited.

Foreign Exchange

It seemed to Einzig that to speak of primitive foreign exchange was apparently a contradiction, since it was the most advanced function of currency. In this case, it is challenging to discuss foreign exchange when dealing with virtual and de-territorialized currencies. But just as he adapted it to include trade between different commodity currencies of various communities (since for a given community, the currency of another is only a commodity and not a currency), a similar effort should make it possible to study the interrelationship of different cryptocurrencies.

"Every money is a commodity outside its *de jure* or *de facto* monetary circulation. The price of one money in terms of the other constitutes the exchange rate."[169] This applies perfectly to cryptocurrencies, not only because there are many markets in which cryptocurrencies are traded against each other and legal tender in different countries, but also because different cryptocurrencies have their spheres of circulation, user communities, and specific utilities. In a later chapter, I will delve into more detail about the

[167] Ibid, 449.

[168] Peter Todd, Luke Dashir, Johnson Lau, Tomoya Ishizaki, Mruddy, Daniel Cousens, et al. "BIP-0065: OP_CHECKLOCKTIMEVERIFY." GitHub, accessed 17 August 2020.

[169] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 459.

utilities and purposes of other cryptocurrencies; for now, it is sufficient to note that there are currencies designed for specific purposes beyond those of Bitcoin.

> In primitive communities we encounter foreign exchange transactions not only between currencies of two communities but also between two currencies used in the same communities. (...) From this point of view we have to differentiate between internal currencies and imported external currencies. Internal currencies are used in the subsistence economy, in addition to being used in domestic non-commercial transactions.[170]

In the case of digital communities, which are not confined to a territory, have pseudonymous identities, and often offer a great deal of anonymity, it is exceedingly difficult to determine the boundaries between communities or who belongs to which one. There are conflicts between communities and within individual communities. The latter can lead to fission into different communities, as well as the forking of the blockchain that the community was using.[171] In addition, the same individual, whether anonymous or pseudonymous, can participate in several simultaneously. Certain communities, however, come into serious conflict with each other, which is commonly referred to in the press as tribalism, using our discipline's terminology.[172]

The scenario of a free money market issued by different actors as one commodity among others had been proposed by F. A. Hayek, a disciple of Ludwig von Mises, in his book*Entnationalisierung Des Geldes* (The Denationalization of Money),[173] has arrived at it uniquely from what he intended. First, neither banks nor financial institutions started issuing these multiple currencies; instead, it was communities. Private entities issue some, but the technology has no intellectual property, and therefore, it belongs to everyone. The second difference is that this has not been done legally or through government decrees establishing the freedom to

[170]Ibid.

[171]See, for example, the Bitcoin block size conflict at Majamalu, "Escenarios Posibles a Partir del Fork," *El Bitcoin* (2017).

[172]See, for example, Michael J. Casey, "Crypto Tribalism Is Holding Back Blockchain," Coindesk (2018). It goes without saying that these "tribes" are not based on kinship ties and do not really have tribal organizations as understood in anthropology. The term refers to a very strong identity as opposed to other identities of the same type only.

[173]Friedrich A. Hayek, *Denationalization of Money, An Analysis of the Theory and Practice of Concurrent Currencies*, (Coronet Books, 1990).

issue their own currencies (*de jure*), but rather outside the law and the government, which then had to adapt to the new scenario (*de facto*).

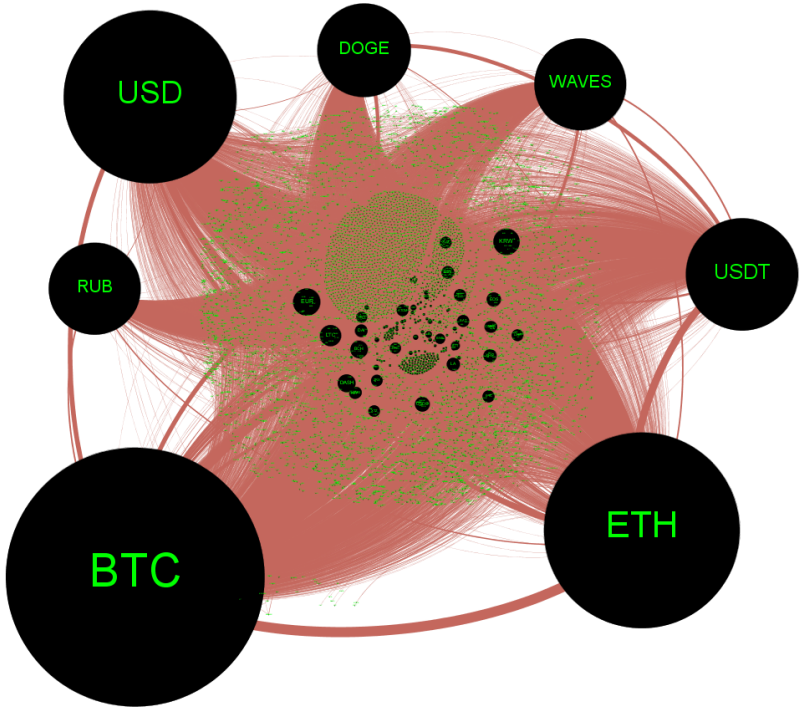


Figure 32: Undirected graph of exchange relationships in cryptocurrency exchanges. Source: own elaboration with data obtained with CryptoCurrency eXchange Trading Library.

> In many instances trade between two communities resulted in either the adoption of the currency of one of the communities by the other or the adoption of some new "international" currency by both.[174]

Figure 34 illustrates the relationships between the various currencies in the market. Each node is a currency, and each connection implies a market pair (and therefore an exchange rate) between them. The size of the nodes is proportional to the number of connections it has, and the

[174] Einzig, Primitive Money in its Ethnological, Historical and Economic Aspects, 460.

thickness of the lines is proportional to the weight of that connection, i.e., the number of times it is repeated in different exchanges (since the information comes from multiple platforms and certain pairs are repeated). The volume traded on each market is not represented. Based on the node size representing Bitcoin, it is evident that it is the most connected of all the currencies and therefore acts as a general intermediary between smaller currencies.

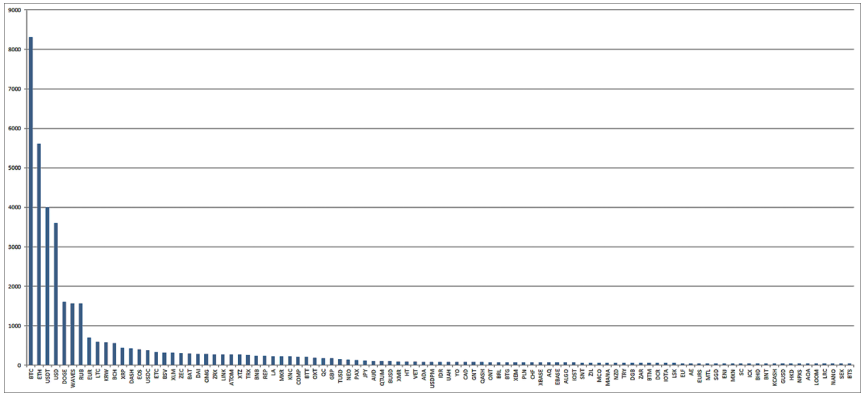


Figure 33: Histogram of the first one hundred currencies with the highest number of connections. Source: own elaboration with data obtained with CryptoCurrency eXchange Trading Library.

Figure 31 illustrates this information graphically, with bars representing the number of connections in descending order. Bitcoin is first, with more than 8,000 connections, followed closely by Ethereum (5,606). Then by the Tether dollar (4005), the US dollar itself (3598), Dogecoin (1604), Waves (1567), the Russian ruble (1564), the Euro (696), where the curvature begins to descend and decrease more progressively. This type of distribution corresponds to the famous "Power Law", which is present in many natural and social phenomena.[175]

Figure 34: Dogecoin (DOGE) isotype.

[175] Reynoso, *Redes Sociales y Complejidad*, 151.

As I have already mentioned, the development of this function is closely related to the measure of value or unit of account, since the values of many currencies are expressed only in Bitcoin; therefore, their value in dollars is affected by fluctuations in Bitcoin. Figure 36 is the transposition of Figure 34. In it, we can see that a substantial number (2,499, 40%) of coins have only one link, 82.30% have seven or fewer links, and 17.70% have more than seven.

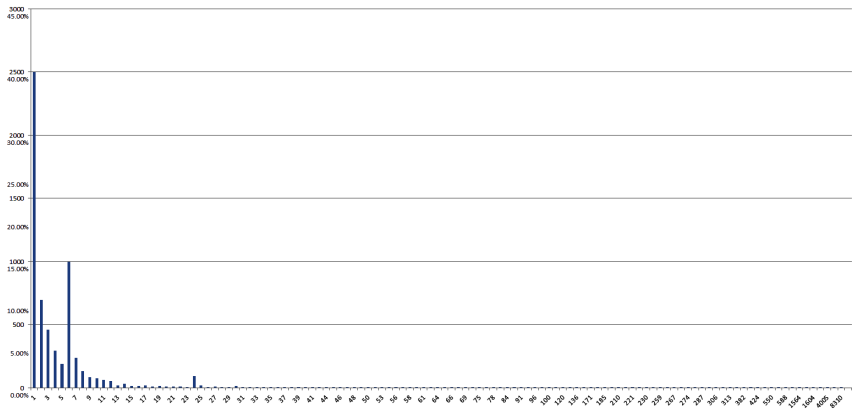


Figure 35: Frequency histogram of number of connections. Source: own elaboration with data obtained with CryptoCurrency eXchange Trading Library.

Table 10: First 8 coins in number and ratio of pairs to coins with only one exchange pair.

TICKER	NOMINAL	PROP.
BTC	899	34%
ETH	236	9%
USDT	263	10%
EUR	195	7%
GBP	23	1%
USD	826	32%
KRW	51	2%
CAD	26	1%

The notion that some currencies only express their values in Bitcoin is not as widespread as it initially appears. Table 10 shows the calculations I have made in this regard. Of the currencies with a single exchange rate or market pair, only 34% have that single pair with Bitcoin as the counterpart. Some 32% have it directly with the dollar, the unit of account. However, in all these analyses, I am only considering the occurrences of each currency in the markets, without taking into account the volumes traded in them. It is possible that the latter also impacts the 'hegemony' of certain currencies over others in the currency market, as the Bitcoin dominance metric discussed above indicates.

In sum, the problem of adopting a common currency in the foreign exchange market can be framed in terms of "Competition and multiscaling in evolving networks," but this paper does not intend to dwell on this point.[176]

◆ Monetary Policy

> …the only way to avoid being driven by continuing inflation into a controlled and directed economy, and therefore ultimately to save civilisation, will be to deprive governments of their power over the supply of money.[177]

This is how F. A. Hayek put it when he advocated transferring the power to issue currency from the hands of governments and central banks to private banks. This was the primary motivation for the cypherpunks in developing forms of digital money, and for Satoshi Nakamoto, who included the headline of the day's newspaper in the first block of the chain, alluding to the financial crisis at the time.[178] In 2020, a tribute was made to that first block in block number 629,999, for which the base money transaction contains the string:[179]

03ef9c0952f09f909f4e5954696d65732030392f4170722f32303230205769746820243222
e335420496e6a656374696f6e2c20466564277320506c616e20466172204578636565647320
2032303038205265736375652020144d696e6564200500ba5e4800

[176] G. Bianconi and A.-L. Barabási, "Competition and Multiscaling in Evolving Networks," Europhysics Letters 54, no. 5. (2001) 436–42.

[177] Hayek, *Denationalization of Money*, 133.

[178] Details are in the *Origin* chapter of this work.

[179] Details can be seen in https://blockstream.info/block/000000000000000000d656be18bb095db1b23bd797266b0ac3ba720b1962b1e?expand

String that is converted to ASCII like this:

ï œŸŸRðNYTimes 09/Apr/2020 With $2.3T Injection, Fed's Plan Far Exceeds 2008 Rescue

It refers to the New York Times headline, "With $2.3 Trillion Injection, Fed's Plan Far Exceeds Its 2008 Rescue."[180]

According to Einzig, "MONETARY policy may be deemed as the attitude of the political authority towards the monetary system of the community under its control."[181] This definition poses some problems for the Bitcoin monetary system, as it is based on the absence of political authority. Does that mean that Bitcoin does not have a monetary policy? Of course not. In fact, its monetary policy is encoded in the software itself and is therefore extremely rigorous. A helpful framework through which Bitcoin's monetary policy can be examined is that of the impossible trinity or monetary trilemma, which holds that only two of these three objectives can be achieved at the same time:

1. to stabilize the exchange rate
2. to enjoy free international capital mobility
3. to engage in a monetary policy oriented toward domestic goals.[182]

In other words, one must always be sacrificed to achieve the other two. For example, maintaining the exchange rate with another currency, such as the US dollar, would require sacrificing monetary autonomy or maintaining strict capital controls. In the case of Bitcoin, the exchange rate is sacrificed to secure the other two goals, hence the volatility of its price.

Einzig does not mention this trilemma scheme because his work dates from the 1940s and 1960s, whereas such a scheme was developed from the 1980s onwards. However, he categorizes monetary policy strategies into types closely related to the impossible trinity. First, it categorizes monetary policy into active and passive attitudes, depending on whether decisions involve implementing measures or refraining from doing so. Throughout this chapter, it should be clear where the Bitcoin protocol actively

[180] Jeanna Smialek and Peter Eavis, "With $2.3 Trillion Injection, Fed's Plan Far Exceeds Its 2008 Rescue," N. Y. Times (2020).

[181] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 464.

[182] Maurice Obstfeld, J.C. Shambaugh and A.M. Taylor, "The Trilemma in History: Tradeoffs among Exchange Rates, Monetary Policies, and Capital Mobility," The Review of Economics and Statistics 87, no. 3 (2005): 423–438.

enforces policy and where it refrains from intervening. Second, it lists the actions covered by a monetary policy.

1. Creation of a new monetary system:
   (a) by decreeing the monetary character of an object or unit;
   (b) by taking practical measures leading to the monetary use of an object or unit;
   (c) by confirming and consolidating, either by decree or by practical measures, the existence of a money developed under private initiative or found in use in a newly-conquered community.
2. Abolition of an existing monetary system:
   (a) by decreeing a change;
   (b) by taking practical measures leading to a change.
3. Alteration or regulation of the functioning of the monetary system:
   (a) by changing the quantity or quality of the unit serving as money;
   (b) by changing the unit of account;
   (c) by changing the volume of money or preventing a change in it;
   (d) by seeking to control prices;
   (e) by seeking to control interest rates;
   (f) by fixing or altering the ratio between several moneys that may exist simultaneously;
   (g) by fixing, altering, or seeking to influence the exchange rate between the local money and outside money;
   (h) by regulating the sphere in which the money is to function.[183]

As most of these actions require the use of coercive or extra-economic means, it can be said that technically, Bitcoin does not implement any of these policies. Regarding point one, Bitcoin was proposed as a unit of monetary value, but not decreed in a legal sense, as it lacks political authority. Point two can be dismissed altogether: although its policy objective is the replacement of another monetary system, it is something it intends to

[183] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 464.

achieve de facto and not through legal imposition. Point three concerns the protocol itself. While 3.a and 3.b can be achieved with a sufficiently broad community consensus, including developers, miners, and users. However, point 3.c is the most fundamental, which is reinforced block after block. As I explained in the Cost of Production chapter, a preset amount of new coins is issued in each block. These coins come out of a so-called 'coinbase' transaction, in which, without any prior input, an output is assigned to an address decided by the miner. That is to say, the miner has the power of decision regarding this primary transaction: although by custom he assigns it to himself as a reward for his work, technically he can assign it to someone else or simply not assign it, thus affecting the issuance.

Then there are the categories into which these policies can fall, which are:

(a) Restrictionist[184]

(b) Stabilizationist[185]

(c) Expansionist[186]

(d) Foreign Exchange[187]

As can be seen from the terms used, the first three items concern the issuance/destruction of circulating currency, and the fourth concerns regulations on the exchange of local currency for foreign currencies. Item d does not exist in Bitcoin, since the protocol does not record information external to the network, such as the price of units in other currencies. It only deals with transactions within the network. Regarding category b, as I mentioned with respect to the trilemma, Bitcoin is not concerned with price stability. Arguably, in this sense, it has a passive attitude towards price instability, given that its design prioritized autonomy and the free flow of capital.

This leaves open the question of whether Bitcoin has an expansionary or restrictive monetary policy with respect to the circulating currency. To address this question, we must revisit the issue of block mining: each block has a reward of new coins that are added to the total circulating currency,

[184]Ibid., 469.
[185]Ibid., 474.
[186]Ibid., 476.
[187]Ibid., 482.

increasing approximately every ten minutes. However, this issue is not always the same; it decreases over time, fractioning in the middle every 210,000 blocks, from its initial value of 50. In other words, from block 0 to 209,999, the reward was 50 bitcoins per block, from block 210,000 to 419,999 it was 25, from 420,000 to 629,999 it was 12.5, and it will continue to decrease until the decimal figures are exhausted and it becomes zero. It is estimated that the total number of bitcoins created at that time will reach 2099999999.9769 or almost twenty-one million. The growth asymptote that the bitcoin circulating currency is programmed to follow after this process can be seen in Figure 37, and in Figure 38, the decreasing evolution of the inflation rate that this process entails. I can therefore affirm that Bitcoin's monetary policy with respect to its circulating currency is restrictive, which causes a deflationary tendency in the price, at least according to the quantitative theory of value. In the section on altcoins, I will discuss different monetary policy implementations.

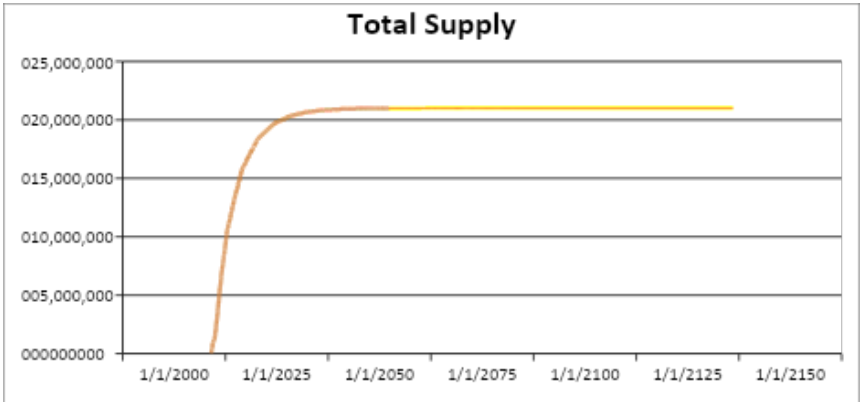


Figure 36: Future Bitcoin supply. Estimated future Bitcoin supply curve, assuming 10-minute blocks. Source: Bitcoin Visuals.

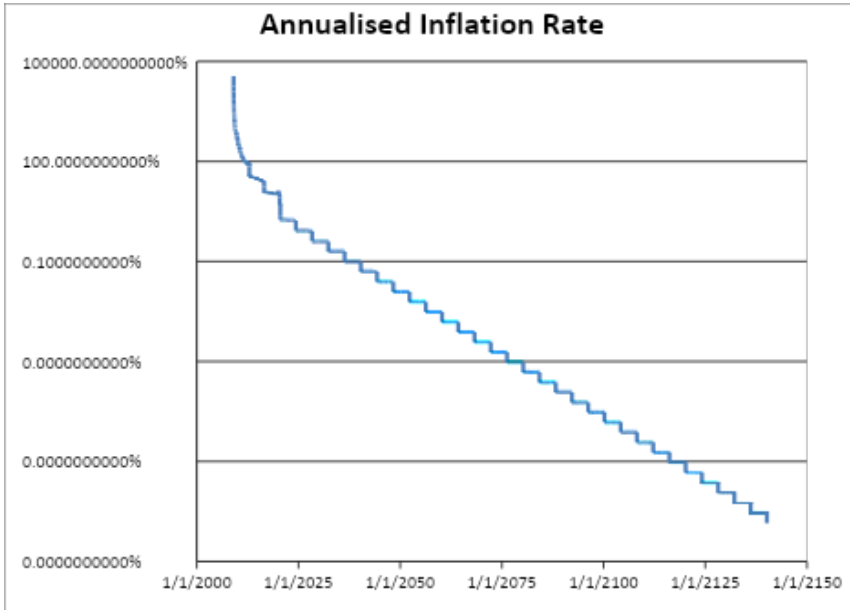


Figure 37: Future Bitcoin supply: Estimation of the future Bitcoin inflation rate curve, on a logarithmic scale, assuming 10-minute blocks. Source: Bitcoin Visuals.

Altcoins

Cryptocurrencies other than Bitcoin are commonly referred to as alternative cryptocurrencies or altcoins. Since the Bitcoin source code is public and not subject to licensing, anyone with sufficient knowledge can modify it and create a different cryptocurrency. That is why all existing cryptocurrencies are, in some sense, another version of Bitcoin, an alternative version, hence the name.

The changes made to these new currencies are, in principle, protocol changes, which primarily imply adjustments to monetary policy. This may then influence the value of their units of account or the economic functions that the system performs, but that is somewhat beyond the developers' control. That is, developers can only address the problems of value and functions through monetary policy. In the following, I will present some of these implementations, their objectives, and how they achieve them.

◆ Privacy-focused Coins (Privacycoins)

The first alternative currencies I will discuss are known as privacy coins, as they are designed to reveal as little information about users as possible. While Nakamoto solved a fundamental problem with Bitcoin —that of achieving a payment system that is both secure and permissionless —he did so at the cost of exposing all transaction information publicly.

Some hardcore cypherpunks were dissatisfied with Bitcoin's limitations regarding privacy (explained in more detail in the chapter on homogeneity) and decided to create other cryptocurrencies that emphasized this aspect. The oldest and most developed of these is Monero, which began in 2014.[1] Bitmonero was first presented on the BitcoinTalk forum.[2] But, given that its technology is the most developed among the currencies I will present, I left it for last.

The year Bitmonero was created, a proposal for another privacy-focused currency, Zerocash,[3] was also published. The technology on which this coin is based is 'zero-knowledge Succinct Non-interactive ARguments of Knowledge' (zk-SNARKs). This technology is initially applied to transactions, ensuring that only the parties involved in the transaction are aware of it, while maintaining the security and decentralization that Bitcoin provides. Just as in Bitcoin, one can prove the holding of a few coins by signing with the last key to which those coins were sent, and that is called a proof of knowledge; zk-SNARKs are arguments of expertise in the same sense. They prove possession (the knowledge of a private key) without revealing what the coins are (the information that the key holds, hence zero knowledge). They are succinct because they can be computed in a genuinely brief time, and they are non-interactive because anyone can use the verification key (which is public) to verify the proof without interacting with the person who generated it. However, not all transactions are hidden in this way. Only shielded transactions are available, but they are optional and not the default method of transferring value in this network.

[1] Monero, "About Monero."

[2] Thankful_for_today, *[ANN][BMR] Bitmonero - a new coin based on CryptoNote technology* - LAUNCHED (2014).

[3] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer and Madars Virza, Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version) (2014).

Figure 38: Monero's (XMR) isotype.

In second place, we have Mimblewimble, presented in 2016 by an unknown author under the pseudonym Tom Elvis Jedusor. According to its author, he chose that name for the mechanism because "it is used to prevent the blockchain from disclosing all users' information."[4] This scheme obfuscates transactions using various privacy proposals made for the Bitcoin network. First, it utilizes confidential transactions (CT),[5] which Monero also employs, and one-way aggregate signatures (OWAS) to merge all transactions in a block into one large transaction.[6] Then he adds one more technology, transaction cut-throughs,[7] and there "We find that we could combine transactions from two blocks, as we combined transactions to form a single block, and the result is again a valid transaction."[8] In short, the entire blockchain is compacted, leaving only the surplus of unspent transactions (UTXOs), saving storage space and providing greater privacy. Bitcoin developer Poelstra published a revised version of the proposal a few months later.[9] The implementation of Mimblewimble was not done in Bitcoin, as proposed by its original author because it would prevent the use of scripts. Instead, it was implemented on two new cryptocurrencies: Grin[10] and Beam.[11]

Lastly, there is Monero, which implements not just one such technology but several, most of them also proposed for Bitcoin. The first of these features is Noether's ring confidential transactions, referred to above, but which contain two parts: on the one hand, ring signatures, whose "...idea therefore is to have the origin pubkey of a transaction hidden in a group of pubkeys all of which contain the same number of coins, so that no one can

[4]Tom Elvis Jedusor, "Mimblewimble." Scaling Bitcoin, (2016).
[5]Shen Noether, "Ring Confidential Transactions," (2015).
[6]Yuan Horas Mouton, "Increasing Anonymity in Bitcoin."
[7]Gregory Maxwell, "Transaction Cut-through," Bitcoin Forum, (2013).
[8]Jedusor, "Mimblewimble."
[9]Amdrew Poelstra, "Mimblewimble," WP Software, (2016).
[10]Quentin Le Sceller, Rodrigo Ferreira, Oliver Simon, and Xavier Lau. "Introducción a Mimblewimble y Grin." 2018.
[11]Beam Foundation, "Beam Position Paper," (2020).

tell which user actually sent the coins."[12] On the other hand, confidential transactions, defined by Gregory Maxwell,[13] also used in *Mimblewimble*. By making use of these two elements, Monero obtains a "A Multi-layered Linkable Spontaneous Anonymous Group signature (…) which allows for hidden amounts, origins and destinations of transactions with reasonable efficiency and verifiable, trustless coin generation."[14]

The second element that Monero uses is stealth addresses as defined by Peter Todd.[15] Instead of signing a transaction to the receiver's address, both parties jointly create a one-time public key, and the transaction is sent there. Only the receiver then has access to those funds using his private key.

Since Monero transaction amounts are private, users have two pairs of keys instead of one as with Bitcoin: one pair for signing transactions, i.e., sending (send key); and one pair for viewing values (view key). From each private key a corresponding public key is derived. Public keys are used to form the address, just as in Bitcoin. The private keys are then used for their respective functions: the send key is used to make transactions with the funds at that address, and the view key clears the transaction values at that address. Thus, one user can choose to show their transactions to another, but the payment system is private by default.

Finally, Monero obfuscates the IP address associated with the transaction issuance. With Bitcoin, the addresses themselves reveal nothing about the users behind them; however, there are several ways to associate them with a real identity. One such way is to track the IP address from which the transaction announcements associated with a given address originate.[16] To make this more challenging, Monero uses two mechanisms. First, clients connect to the internet through the TOR[17] and I2P networks,[18] which

[12]Noether "Ring Confidential Transactions," 3.

[13]Gregory Maxwell, "Confidential Values," (2015).

[14]Noether "Ring Confidential Transactions," Abstract.

[15]Peter Todd, "Stealth Addresses," SourceForge, (2014).

[16]That is: if I send a Bitcoin transaction from my computer, that transaction could be associated with my IP address at the time and my internet provider can reveal my real identity.

[17]TOR, The Onion Router, is a protocol and network for obfuscating web traffic. Thousands of volunteer computers form a network in which TCP/IP packets travel from one end of the communication (client and server) to the other, passing through several intermediaries, covered with several layers of encryption, like an onion. See Roger Dingledine, Nick Mathewson, and Paul Syverson Tor: *The Second-Generation Onion Router*, (Defense Technical Information Center , 2004).

[18]"I2P: Un Sistema Escalable para las Comunicaciones Anónimas."

are designed to mix traffic and hide clients' and servers' identities and locations. Secondly, it uses the Dandelion++ protocol. Students at the University of Illinois developed the dandelion protocol. Its operation is explained as follows:

> Dandelion spreading consists of an anonymity phase and a spreading phase (…). In the anonymity phase, the protocol spreads the message over a randomly-selected line for a random number of hops; in the spreading phase, the message is broadcast using diffusion until the whole network receives the message. [19]

In other words, instead of publicly announcing the transaction, the originating node initially announces it only to a few randomly selected nodes and then broadcasts it to all nodes simultaneously, thereby obfuscating its origin. The improved version, called ++, was proposed the following year.[20]

To summarize, Monero employs multiple techniques simultaneously to conceal the origin, destination, and number of transactions, as well as the geographic location of users and the relationships between transactions associated with the same key. Privacy-focused currencies do not aim to implement a different monetary policy from Bitcoin but rather to better conceal user information, which may impact, as I explained above, the homogeneity of monetary units.

◆ Proof of Stake

Proof-of-stake is a consensus mechanism that replaces the proof-of-work mechanism. It is not an altcoin per se, but rather a component of the consensus mechanism, and several coins can utilize it. The premise is that instead of mining by solving a cryptographic riddle and finding a hash for the block below a certain value, blocks are validated by a kind of stake.

[19] Shaileshh Bojja Venkatakrishnan, Giulia Fanti, and Pramod Viswanath, "Dandelion: Redesigning the Bitcoin Network for Anonymity," (2017), 8.

[20] Giulia Fanti, Shaileshh Bojja Venkatakrishnan, Surya Bakshi, Bradley Denby, Shruti Bhargava, Andrew Miller, and Pramrod Viswanath, . "Dandelion++: Lightweight Cryptocurrency Networking With Formal Anonymity Guarantees." *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 2, no.2 (2018), 1-35.

The first algorithm of this type was proposed very early, for a coin called PPCoin, which is now known as PeerCoin.[21] The primary goal was to minimize the substantial energy expenditure associated with proof of work. To this end, a way of securing transactions was sought that would not require such a large number of calculations but would be just as secure. In this sense, a betting mechanism was proposed. Miners put their coins in play to guarantee the validity of the blocks. They are punished by losing their guarantee if they bet on an invalid block. On the other hand, if they collaborate by supporting valid blocks, they receive a reward.

The first consequence of this system is that it gives rise to a feedback mechanism, in which players with the most coins at stake receive the most, resulting in exponential growth. In the PPCoin proposal, a valid block is reached by finding an appropriate hash, but the space of hashes is inversely proportional to the total coin age. This coin age considers the number of coins and the time that has elapsed since their creation. The coin age value is calculated by multiplying the number of coins by the age. Thus, those with the oldest coins have the best chance of finding the block. The transaction in which the reward is collected destroys this accumulated age at the same time as the reward is granted, so capital does not accumulate exponentially. A few players become disproportionately powerful at the expense of everyone else. This accumulation is not only avoided for ethical or moral reasons, but also because it functionally harms the system: as in the proof-of-work consensus, an actor with a majority position in deciding valid blocks can engage in fraud in the well-known 51% attack. Another problem this consensus mechanism entails is that it does not provide an incentive to maintain a single blockchain, i.e., to avoid forks. In proof-of-work consensus, it is in the best interest of miners to focus all their mining power on a single chain. In contrast, in proof-of-stake, multiplying the number of networks an actor has their stakes in is, in fact, beneficial, as it doesn't require extra work to maintain them.

[21] Sunny King and Scott Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," (2012).

◆ Ethereum and Smart Contracts

Szabo introduced the concept of contracts between parties enforced by software rather than by an authority in 1997,[22] as part of the cypherpunk arsenal being developed at the time, but with no practical application at the time.

It was not until 2013 that Buterin published a document presenting a future implementation of this concept,[23] which is now the foundation of what is now the second most important cryptocurrency, Ethereum, launched in 2015. In this document, Bitcoin is presented as a state machine (each block being a state), in which one goes from one to another by means of transactions. With the caveat that:

> …the state is not encoded in the block in any way; it is purely an abstraction to be remembered by the validating node and can only be (securely) computed for any block by starting from the genesis state and sequentially applying every transaction in every block.[24]

In addition to this, he acknowledges that Bitcoin already has a contractual capacity due to the language it uses, script or Bitcoin script:

> A script is essentially a list of instructions recorded with each transaction that describe how the next person wanting to spend the Bitcoins being transferred can gain access to them.[25]

This ability to condition transfers of value is fundamental to contracts; however, the language Bitcoin uses to achieve this is limited. It is not Turing-complete,[26] it does not allow loops in one of these algorithms, and transactions only support binary states (they are, or are not, spent; spending only part of it involves creating one UTXO with the actual spend and another with the "return"). Moreover, transactions are blind to their metadata (which goes in the block header) and their value outside the system.

Ethereum, on the other hand, aims to,

[22] Nick Szabo, "Formalizing and Securing Relationships on Public Networks" First Monday, (1997).

[23] Vitalik Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," (2013).

[24] Ibid. Mining.

[25] Bitcoin Wiki s.v. "Script."

[26] On the different types of formal languages and their level of complexity, see Wikimedia Foundation, "Chomsky Hierarchy."

> … building what is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions.[27]

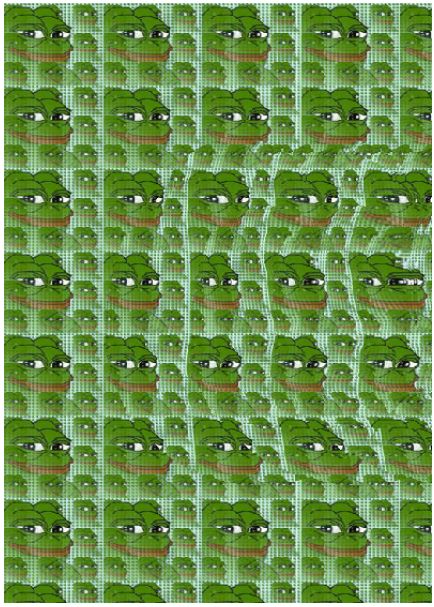


Figure 39: "Magicpepeye", a rare Pepe, which were the first non-fungible tokens. Made directly on the Bitcoin network. Source: HYPERLINK "http://rarepepedirectory.com/?p=188" Rare Pepe Directory.

In other words, Ethereum is a network of computers that functions like a large computer, where applications or programs created freely by users are developed. Instead of addresses, as in Bitcoin, Ethereum has accounts. These accounts can be of two types: external accounts, held by a user with a private key (as in Bitcoin), and contracts, accounts controlled by the instructions given to them. The language in which the instructions are written is called EVMC, which stands for Ethereum Virtual Machine Code.

Ethereum transactions share the same elements as Bitcoin transactions or any other cryptocurrency: recipient, signature, and number of coins transferred. In addition, they have different parameters: an optional information field, in which you can put anything, a STARTGAS field where the maximum number of computational operations allowed for that transaction is stipulated, and a GASPRICE field with the fee to be paid per computational step. These last two parameters are not, as in Bitcoin, to ensure the transaction's priority in the event of network saturation and to encourage miners, but are even more critical. Since it is a Turing-complete language, this mechanism prevents

[27] Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum.

the system from falling into an infinite loop, a phenomenon known as the *Entscheidungsproblem* (decision problem).[28] The supercomputer will stop the execution of an algorithm when it runs out of gas, so it cannot get stuck in an infinite loop. Gas is a unit of account equivalent to one computational step or 0.2 bytes of information, and its amount is translated into ether (ETH), the network's native currency. Thus, a transaction has a cost relative to the number of steps required to resolve it and the weight of the information transmitted.

Unlike Bitcoin, Ethereum's blockchain contains transactions and the current state of the network, including all accounts and their respective balances.[29] In addition, Ethereum blocks are mined every 4-15 seconds on average, compared to 10 minutes for Bitcoin. Therefore, the size of the Ethereum blockchain is much larger than that of Bitcoin.

Many applications have been developed on this virtual machine. One of the main advantages is the possibility of creating currencies other than ether, native to the network, allowing for many different currencies within Ethereum. In addition to coins, fungible units, equivalent to each other, there are non-fungible tokens (NFT) that represent or are in themselves a unique object, such as a collectible object, a title that describes the possession of a material or immovable asset, etc. Another of the most important uses is the development of decentralized applications or dApps, which are, as the name suggests, applications, pieces of software, that instead of depending on a server, run on the blockchain: casinos, markets, video games, betting schemes, financial derivatives, identity and reputation systems, contests, etc.

The development of such applications gave rise to DeFi. The primary concept of DeFi is that the entire web of financial institutions and services can be recreated in decentralized applications. Trying to analyze the phenomenon in depth would require a significant amount of space and seems unnecessary, as it is only in its initial stages. Therefore, I will simply point out a few use cases to illustrate. One especially useful way to un-

[28] D. Hilbert and W. Ackermann, Grundzüge der Theoretischen Logik (Die Grundlehren der Mathematischen Wissenschaften vol. 27, 1949), 94.

[29] The current state is not copied completely in each block, but only the differences with respect to the previous block or changes. All parts that remain the same are referenced in previous blocks by hash pointers organized in a structure similar to Merkle trees called Patricia trees, defined in Donald R. Morrison, "PATRICIA—Practical Algorithm To Retrieve Information Coded in Alphanumeric," *Association for Computing Machinery* 15, no. 4 (1968), 514–34 and in Konstantin Knizhnik, "Patricia Tries: A Better Index For Prefix Searches," Dr. Dobbs, (2008).

derstand how this works in practice, without going too deeply, is through the example of a user who made a trade with a $16,000 profit in a single block.[30] As the article mentioned above explains, the operation consisted of four transactions on different platforms, in which this user: borrowed a loan (flash loan) in one currency, exchanged it for another on one market, exchanged it back on another market (taking advantage of the price difference on both platforms, an operation known as arbitrage), and then repaid the loan with interest, keeping the difference. This flash loan was taken and repaid within the same block, allowing the operation to occur simultaneously. In short, DeFi enables various financial operations, including managing loans, creating decentralized exchanges (DEX) and automatic market makers (AMM),[31] leveraging, arbitrage, and participating in investment funds, on different interrelated platforms operating on the same blockchain.

◆ Stablecoins

Stablecoins are cryptocurrencies designed to maintain a constant price over time. The reference price is typically the US dollar, and various approaches are employed to achieve parity with this currency. Regarding monetary policy and the impossible trinity, the fixed exchange rate is prioritized over the other objectives.

The first of these is the most widely used and employs the simplest scheme. It is called the Tether Dollar.[32] It relies on a private company that holds a reserve in dollars presumably equal to the number of cryptocurrencies it issues; that is, it is a cryptocurrency backed by legal tender. The problems this solves are mostly legal, as it does not use real dollars but rather a substitute, which was its purpose. In all other respects, it is a currency that does not need a blockchain since a private company manages it. By achieving a fixed exchange rate with a reserve, they sacrifice a fixed money supply to keep the price stable, as it is constantly fluctuating. In addition to the Tether dollar (USDT), other companies have created their own digital dollars, such as USD Coin (USDC) and

[30] Nicolás Antiporovich, ""DeFi Madness: One Person Earned 16,000 USDC in 13 Seconds with a Flash Loan," *CriptoNoticias-Bitcoin, Blockchains and Cryptocurrencies*, (2020).

[31] Hayden Adams, Uniswap Whitepaper." HackMD (2018).

[32] Tether, Tether: Fiat currencies on the Bitcoin Blockchain, (2016).

TrueUSD (TUSD), which are part of a suite of cryptocurrencies backed by legal tender: TCAD, TAUD, TGBP, and THKD. These types of assets can be referred to as centralized stable cryptocurrencies.

Other projects went further and tried to create a stable value cryptocurrency in a decentralized way. The first to achieve it on a large scale is MarkerDAO's DAI.[33] As their paper details, Dai is a stablecoin that, like those mentioned above, is equivalent to one US dollar. Yet, that value is derived not from dollar reserves held in certain bank accounts, but from the operation of various smart contracts on the Ethereum network that manage a backing in other cryptocurrencies.

> Users generate Dai by depositing collateral assets into Maker Vaults within the Maker Protocol. This is how Dai is entered into circulation and how users gain access to liquidity. (…) Every Dai in circulation is directly backed by excess collateral, meaning that the value of the collateral is higher than the value of the Dai debt (…). A collateral asset is a digital asset that MKR holders have voted to accept into the Protocol. (…) generating Dai does create an obligation to repay the Dai, along with a Stability Fee, in order to withdraw the collateral leveraged and locked inside a Vault.[34]

In other words, the Dai currency is issued as a loan and destroyed when repaid. According to its document, Dai is capable of fulfilling several of the monetary functions listed above: store of value, since being stable it tends to maintain the purchasing power of its holder; medium of exchange, since it acts as a digital dollar without bureaucratic barriers; medium of deferred payments, since the protocol is a credit system and is also widely used in the growing DeFi ecosystem; and unit of account, at least within its system and across DeFi, since the reference price is actually the US dollar.

Another stablecoin is DoC, Dollar on Chain, which is part of a larger system called Money on Chain. The latter is a protocol built on smart contracts, similar to Maker, except that, unlike Maker, these contracts are not created on the Ethereum blockchain but on RSK. RSK (derived from "rootstock" and "rhizome") is a sidechain to the Bitcoin blockchain, developed by RSK Labs, a technology company founded by Sergio Lerner, a graduate of the University of Buenos Aires.[35] RSK is, then, a separate

[33]Maker Foundation, "The Maker Protocol White Paper," (2020).
[34]Maker Foundation, "The Maker Protocol White Paper."
[35]Lerner "Rsk.," 15.

chain that interacts with the main Bitcoin chain, i.e., it is a second layer of the blockchain. To transfer bitcoins (BTC) from one chain to the other, they are sent to a vault address, where they are frozen, and an equal number of bitcoins is issued on the RSK chain, known as Smart Bitcoins (RBTC). Conversely, returning the bitcoins to the main chain destroys the RBTC and releases the original bitcoins from the vault address. This second layer aims to bring Ethereum-like smart contract functionality to Bitcoin.[36]

Using these contracts, the Money on Chain (MoC) protocol,[37] was developed, which enables the production of a stablecoin called Dollar on Chain (DoC), also anchored to the dollar's value. Unlike DAI, the collateral backing the DoC is not a basket of other cryptoassets but leveraged positions in the price of RBTC that expire every 30 days.[38] DoCs are issued upon depositing RBTC into the protocol, and interest is charged upon cancellation,[39] just like DAI. The other two MoC tokens are BitPro and BTCX. The protocol also features an integrated decentralized exchange or marketplace (DEX) where these assets are traded. BitPro is issued in exchange for RBTC loaned to the protocol and earns interest at a variable rate for transferring the volatility of the Smart Bitcoins to the BTCX token. BTCX, on the other hand, are leveraged RBTC positions on the DEX, which operate like a futures contract and expire after 30 days; they are not transferable. An interest rate is paid to use RBTC.

In short, the MoC protocol allows holders of smart bitcoins to exchange them for any of three assets according to their preference: a leveraged position, a floating-rate loan, or a stable-price currency. The three assets are interdependent. This interrelationship transfers the price volatility of BTC to the BTCX token, producing DoC, a currency with an exchange value equivalent to one US dollar.

[36] Ibid., 8.

[37] Maximiliano Carjuzaa, Alejandro Bokser, and Javier García Sánchez, "Money On Chain: Protocolo de una Stablecoin Colateralizada con Bitcoin," (2019).

[38] Ibid., 2.

[39] Ibid., 3.

◆ Social Cryptocurrencies

As is evident, the political philosophy behind Bitcoin and that of social currencies are quite different. This topic is well- developed in Peyrouzet's thesis for the University of Exeter, so there is no need to delve into it here.[40] Instead, I will focus on some cryptocurrency implementations that address issues arising in the development of social currencies or tackle similar problems.

First, as I explained above, blockchain technology's greatest achievement is finding a solution to the Byzantine Generals Problem. It has thus achieved a type of system that can reach an agreement even with little or no trust between its parties. This is a problem that solidarity markets faced, even if they did not put it in those terms. The blockchain solves the problems of counterfeiting, manipulation, lack of transparency, centralization, and consensus at different scales. As the examples in the section on them make clear, such problems are common in social currency systems. With a cryptocurrency, there is no need for coordinators to verify the authenticity of transactions; the issuance of monetary units is easily verifiable by the entire community, and counterfeiting is next to impossible.

However, other problems persist, and new issues are affecting cryptocurrencies. If we examine the functioning of the first Barter Club in Quilmes, before printing its currency, credit consisted of the goods each member brought to a meeting, valued in pesos or dollars. From Moini's perspective, we have a unit of account, the peso, but separate from the recording device, the notes. Since each member has a value that is taken in and out, it is recorded in a general spreadsheet. Goods are exchanged according to their equivalence in price, but without a finite number of currency units circulating as another good. Blockchains have not yet succeeded in decentralizing this accounting system, which requires conceiving money endogenously, as a credit generated by contributing goods and cancelled by subtracting them. Current consensus mechanisms view currency as an a priori-produced good that mediates exchanges between other a priori-produced goods, independent of one another. The proof-of-work is

[40] Peyrouzet García-Siñeriz, "In Blockchain They Trust – Now, Power to the People or to the invisible Hand? An Analysis of the Ideological Tensions and Affinities Between Crypto-libertarian and Crypto-commonist Visions, Projects and Aspirations for the Blockchain Revolution."

a function of computing power, and the proof-of-stake is a function of risked capital. I am only aware of one cryptocurrency that has made progress in this regard, and it will be detailed towards the end of this chapter.

Gómez outlined four factors that make governance systems sustainable and compared the cases she analyzed along these four dimensions. I added cryptocurrencies as an extra case to this comparison.

Table .1: Table 11: Sustainability of governance systems. Taken from Gómez and expanded.[41]

	Input legitimacy	Rule enforcement	Resource synergies	Transaction costs	Organization costs
RGT	Low	Low	Low	High	High
ZO	Reasonable	Reasonable	High	Low	Reasonable
RTS	High	Reasonable	Low	Low	Low
LOCAL	High	High	Low	Low	Low
CRYPTO	Reasonable	High	High	Low	Low

1. Input legitimacy: To what extent does the process of rule definition help to win acceptance? The focus is on the process of rule-setting for non-state currency systems and the replication of nodes, besides factors like idealism and common values.

2. Enforcement: To what extent do institutional mechanisms of monitoring and enforcement operate? The focus is on ways to obtain effective compliance of rules, even against some resistance.

3. Benefits (in relation to output legitimacy): To what extent is resource synergy achieved to deliver results, solve problems and resolve conflicts? The focus is on management of scarce resources and activities in common to support the income-generation efforts of households.

4. Transaction and organizational costs (in relation to output legitimacy): to what extent are risks and uncertainties minimized? The focus is on the uncertainty of trading with means of payment accepted voluntarily – the *créditos* – with the risk of loss of value. To what extent are the costs of sustaining self-organization minimized?

[41] Gómez, *Argentina's Parallel Currency: The Economy of the Poor*, 129.

> The attention is on the costs of decision-making in each governance system.[42]

The advantages of cryptocurrencies in this respect are clear: the protocol is not only enforceable but also automatic, reducing operational costs and making rule enforcement higher than in any other case. On the other hand, this impacts transaction costs. Following Coase,[43] Dahlman separates the transaction costs into three categories: "search and information costs, bargaining and decision costs, policing and enforcement costs."[44]

It is on the third of these costs that one must dwell and note that any currency carries that cost in some form, as monitoring and enforcement are not actions that the participants in the transaction carry out but usually a larger body such as a police force, a government, a court or the community itself. That is why blockchain technology, and by extension smart contract technology, by making enforcement automatic and not requiring an external force for this, lowers both the operational cost of the system (which is ultimately also more transparent, since it is the consensus mechanism, usually mining, that performs this function) and the transaction cost for participants.

One consensus mechanism proposed specifically for social currencies is Faircoop's, proof-of-cooperation,[45] implemented in its FairCoin.[46] The problems it aims to solve are the energy expenditure resulting from the proof-of-work and the speed of block creation, which impacts the time it takes for transactions to be verified. The circulant is a fixed amount, which is plausible to be modified only in implementations other than the leading Faircoin network. Consensus is not open, but between cooperatively validated nodes, a function akin to barter club coordinators is established, which restores trust to individuals and the community rather than relying on the protocol, i.e., it departs from the principle of trustlessness. The community also sets the price, committing to accept a certain exchange rate to avoid the high volatility to which most cryptocurrencies are subject, whose prices depend entirely on market mechanisms. Faircoin was

[42]Ibid., 112.

[43]R. H. Coase, "The Nature of the Firm," Economica 4, no. 16 (1937), 386–405.

[44]C.J. Dahlman, "The Problem of Externality." *The Journal of Law and Economics* 22, no. 1 (1979): 148.

[45]Enric Duran, Thomas König, and Roland Alton Niklas Fessler, "The Proof-of-Cooperation Blockchain FairCoin", (2018).

[46]Ibid., 7.

implemented by the Faircoop cooperative and created a series of marketplaces, but it faced the same problems of factionalism and power bidding that appeared in barter networks, which primarily impacted the ability to maintain a stable price for the currency.[47]

Other cryptocurrencies incorporated a rusting mechanism inspired by Silvio Gesell, as in the case of Venado Tuerto, from the chapter on social currencies. One is Freicoin,[48] whose name references Gesell's *freigeld*. The currency has a mechanism in its protocol whereby those who keep it stored pay a 5% annual fee, which is distributed to the rest of the users, to promote circulation and discourage hoarding. Another cryptocurrency that applies this idea is Bitgesell,[49] or at least pretends to, as it technically works like Bitcoin, but 90% of each transaction fee is destroyed, preventing the hoarded circulating currency from losing value. Still, the opposite progressively reduces it asymptotically and increases its value.

Finally, the MonedaPAR coin was developed at the University of La Plata. According to its website:

> MonedaPAR is a mutual credit system for the exchange of goods, services and knowledge based on Blockchain technology (...) Each transaction is recorded in the system as a positive PAR balance for the selling prosumer and as a negative balance for the buyer. The system works using overdrafts: each prosumer joining the system starts with a zero PAR balance and those who receive an endorsement from a previous member of the network can access an overdraft limit - negative balance - to buy products without having previously accumulated PAR. These credits do not carry an interest rate (...) All members commit to try, over time, to pay off their negative balances by selling their own products to achieve balanced PAR balances. In this way, over time all participants tend to take from the community an amount of wealth equivalent to what they give. (...) PAR does not function like traditional "money" or other financial assets. It functions only as a medium of exchange within the network and serves to keep track of how much value - work - has been given and how much has been received. The fact that someone has a negative PAR balance necessarily implies that another member of the system has a positive one. Therefore, the sum of all balances

[47] Talk Alternatives, About Mutual Credit Systems, Cryptos & the FairCoop Community - with Guy James, (2020), 25:20.

[48] Mark Friedenbach and J Timón, Freicoin (2015).

[49] Wu-emma, Bitgesell.

> is always zero. There is no net financial wealth within the system. (...) the Argentine peso is used as a unit of account - as a reference for determining prices - but not as a backing.[50]

Regarding technical aspects, $PAR is a currency of the BitShares network:[51] specifically the DEX blockchain, which exchanges different cryptocurrencies and is itself a blockchain that allows assets with programmable functions, similar to smart contracts, to be created.

Regarding its theoretical foundations, they explain the following:

> Mutual credit currencies are based on Silvio Gesell's idea that the sole purpose of money should be to enable communities to make the most of their productive capacities, facilitating the exchange of goods in a safe, quick, and inexpensive way. Whenever money is used as a means of saving and not as a means of exchange, it tends to be withdrawn from circulation and its scarcity proves to be an obstacle to the reciprocal exchange of wealth. (...) Gesell, therefore, suggested a type of currency whose circulation should be compulsory or at least strongly stimulated, for example, through rusting. Another way of generating this incentive is mutual credit systems. (...) Currencies based on mutual credit are part of the universe of so-called complementary currencies. In general terms, complementary currencies are agreements between the members of a community to accept as a medium of exchange a currency that is not legal tender.[52]

MonedaPAR has a strong community and interpersonal anchor, more typical of social currencies than cryptocurrencies, and a well-established governance system:

> The government of *Moneda Par* functions at the national level as a Federation of Nodes. This Federation is composed of four members of the founding team and one representative from each of the nodes. (...) The Federation authorizes the creation of new nodes, which is implemented by sending a guarantee to the node's administrative account. (...) The Nodes have the autonomy to define, through regulations, the use given to the currency and the way in which it is implemented. The governing body of each Node can define the conditions of access to the service for each of its members. (...) The

[50]"Funcionamiento del Sistema." *Moneda Parn*.
[51]"BitShares Documentation," BitShares Blockchain Foundation, (2019).
[52]"Fundamentos Monetarios," Moneda Par.

> only aspect over which the governing body of the Node does not have autonomy is the issuance of currency. The issuance decisions, implemented through the granting of guarantees, must be agreed with the Federation. This is because, based on lessons learned from other historical experiences, monetary imbalances in one node can quickly spread to the others. Also, the Node administration account is itself an account whose overdraft level is defined in consensus with the Federation. (...) Legally, *Moneda PAR* is a system of payment orders and/or discounts registered with INAES by the *Asociación Mutual Conexión*. To make use of the system, it is necessary that the interested parties either join the mutual association or form a new mutual association that signs an agreement with *Conexión*.[53]

It is evident from the above that MonedaPAR is, in many ways, a continuation of the social and complementary currencies project that developed in Argentina during the 1990s and 2000s. It leverages certain successful practices, including decision-making by consensus and federated organization of nodes and regions. It incorporates recent technology to compensate for shortcomings (excessive issuance, lack of transparency, counterfeiting). As I anticipated at the beginning of the chapter, this type of credit payment system is an essential advance in the development of cryptographic social currencies and of all cryptocurrencies in general, but MonedaPAR has not yet managed to consolidate such a mechanism directly in the software; it depends to a large extent on interpersonal contact, trust, its organizational structure, and the country's legal framework to enforce its rules.

[53]"Forma de gobierno," Moneda Parn.

Part 3

Final thoughts and conclusion

Conclusion on the Taxonomy of Monetary Instruments

At the beginning of the second part of this thesis, I posed two problems to be addressed: to define whether Bitcoin is a monetary instrument and to determine its place in the taxonomy of monetary instruments. Based on everything I have said in the section on Bitcoin, I can answer the first question affirmatively. Following Moini's definition of a currency or monetary instrument, Bitcoin is an instrument that can record and transmit information about monetary rights, thereby serving as a currency.

Answering the second question is problematic, since the conceptual framework used by the taxonomy presented by Mises, and widely accepted in economics, is confined to the metallic paradigm. On the one hand, no distinction is made between currency and money. This problem is easily solved; a mere change of terminology allows us to establish that what Mises calls 'money' refers specifically to what, following Moini, I here refer to as 'currency'. The term 'money' is reserved for a more abstract and invariable concept that has already been explained. On the other hand, Mises's taxonomy presents us with greater difficulty in classifying certain phenomena, such as cryptocurrencies or Wicksell's ideal banking. This difficulty arises from the fact that one of its fundamental assumptions is that credit is a derivative of the medium of exchange, namely, currency. Wicksell's ideal banking also fits into this paradigm, consisting of a credit currency derived from immobile reserves.

Nevertheless, I consider that Mises's scheme ains helpful and can be adapted to Moini's theory of money and credit with minimal modifications. The examples of the barter club and MonedaPAR can be classified as currency-credit, even if this credit is not derived from a medium of exchange, but directly from commodities. Conversely, cryptocurrencies

present a greater degree of difficulty in their classification. It is easy to dismiss them as a credit-currency, given that they are not produced as such: the credit-currency, although preceding the commodity-currency as a medium of exchange, arises from exchange, as a unit of account or standard, as Moini explains. This is not the case with Bitcoin, but rather with other cryptocurrencies designed specifically for this purpose, such as MonedaPAR. We have already seen how it is problematic to classify Bitcoin as a commodity-currency, because it has a relative production cost and lacks a prior use value as a non-monetary commodity. From an individual's point of view, Moini points out that Bitcoin can be considered a good, but neither a consumer good nor a production good; it is merely a good for the exchange and storage of value. This item occupies a token-currency category, which it shares with legal tender (as elaborated by Knapp) and with certain types of social currencies (classified as fiat by Hirota). In Figure 41, I present a reworking and extension of Mises'ss taxonomy, which includes cryptocurrencies of the Bitcoin type, certain forms of social currency presented in the corresponding chapters, and legal tender. Commodity currencies, extensively documented and compiled by Einzig, remain in the same category. The currency substitutes also stay in their places.

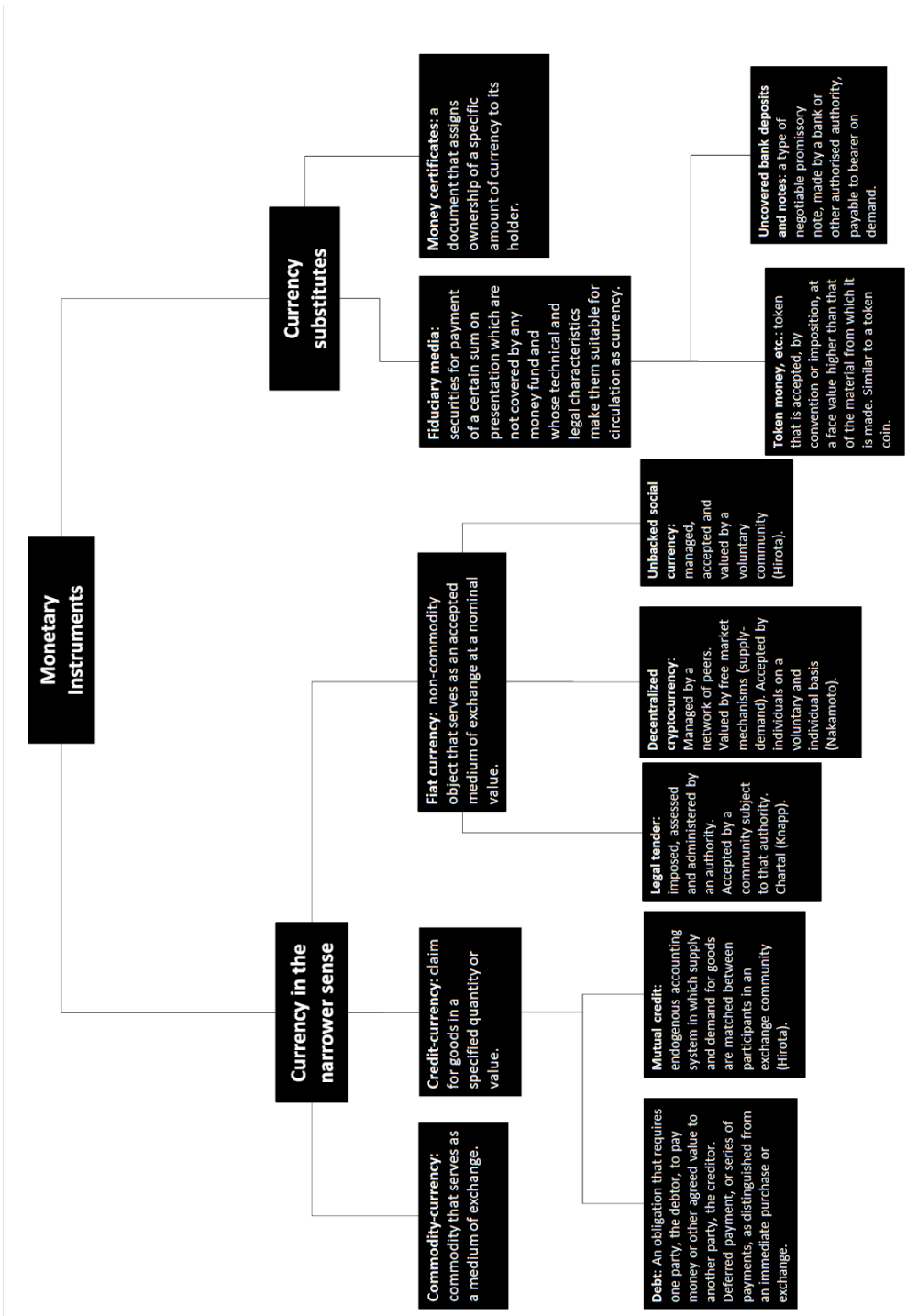

Monetary Instruments
Currency substitutes
Money certificates: a document that assigns ownership of a specific amount of currency to its holder.
Fiduciary media: securities for payment of a certain sum on presentation which are not covered by any money fund and whose technical and legal characteristics make them suitable for circulation as currency.
Uncovered bank deposits and notes: a type of negotiable promissory note, made by a bank or other authorised authority, payable to bearer on demand.
Token money, etc.: token that is accepted, by convention or imposition, at a face value higher than that of the material from which it is made. Similar to a token coin.
Currency in the narrower sense
Fiat currency: non-commodity object that serves as an accepted medium of exchange at a nominal value.
Unbacked social currency: managed, accepted and valued by a voluntary community (Hirota).
Decentralized cryptocurrency: Managed by a network of peers. Valued by free market mechanisms (supply-demand). Accepted by individuals on a voluntary and individual basis (Nakamoto).
Legal tender: imposed, assessed and administered by an authority. Accepted by a community subject to that authority. Chartal (Knapp).
Credit-currency: claim for goods in a specified quantity or value.
Mutual credit: endogenous accounting system in which supply and demand for goods are matched between participants in an exchange community (Hirota).
Commodity-currency: commodity that serves as a medium of exchange.
Debt: An obligation that requires one party, the debtor, to pay money or other agreed value to another party, the creditor. Deferred payment, or series of payments, as distinguished from an immediate purchase or exchange.

Figure 40

The Philosophy of Cryptographic Money

This final section presents reflections and conclusions based on the material presented throughout this study. As in the section devoted to Bitcoin, the outline used is that of Einzig's book. In the same way that in the second part I approached Bitcoin from different perspectives with which he approached what he called primitive money, the last part of his work was devoted to reflecting on specific questions related to the development of a social theory of money and the process of substitution of primitive for modern money that he was observing. Building on that analysis, I dedicate this final part to reflecting on Bitcoin in the same aspects and on the process of integration or substitution it is undergoing with respect to the modern form of currency, which at the time replaced the other, labeled as primitive.

◆ Economic (and Political) role

While trying not to fall into a position of unilinear evolutionism, I will agree with Einzig that:

> Primitive races could not be expected to jump the intermediate phases between barter and scientifically managed credit money merely because by some freak chance or anachronism a genius born long before his time happened to strike upon the idea of it. The "inevitability of gradualness" has to be regarded as a basic principle in monetary evolution.
>
> This does not mean that at every period the monetary system necessarily corresponded to the stage of evolution of that period.[1]

This insight suggests that cryptocurrencies will not establish themselves suddenly, but only to the extent that social relations are suitable for this type of currency. In this sense, Bitcoin is not ready to fulfil the key role of a monetary instrument ("a device for recording and transmitting information about monetary rights") in several respects:

- On a technical level, the number of transactions that the network can process (approximately 2,500 every 10 minutes) is significantly lower than that of other payment systems, whether electronic or physical.
- On a social level, very few people are familiar with or have a sufficient incentive to use Bitcoins on a daily basis.
- At the economic level, it cannot satisfactorily fulfill some key functions: medium of exchange and unit of account.

Apart from this, Einzig draws attention to another social effect of the currency:

> …the adoption of money economy even in its primitive form tended to obscure the effects of inequalities in wealth and income. (…) Once wages and profits came to be earned not in actual goods intended for direct consumption but in money, the recipients were no longer in a position to know precisely or even approximately what they were receiving in terms of real goods and services. It depended on the way they used their money and on the prices they had to pay. (…) So long

[1] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 485.

> as primitive currency consisted of commodities with full intrinsic value its employment did not materially obscure the true picture of distribution. With the adoption of ornament money, however, the situation changed, and the further monetary system progressed towards modern money the more it obscured distribution.[2]

To what extent Bitcoin or other cryptocurrencies can counteract or accentuate this trend is debatable. On the one hand, Bitcoin was initially presented as a solution to the abuses of power by core players in centralized monetary systems. A decentralized system without authorities does not permit artifices such as quantitative easing, the freezing of funds for third parties, and other forms of transferring wealth from one sector of society to another by those who exercise decision-making power over monetary policy. On the other hand, their pseudonymous and quasi-anonymous nature greatly facilitates the concealment of large fortunes, allowing influential market players to abuse their position without accountability. In my view, the benefits outweigh the detriments that the widespread use of such a system can bring compared to the centralized systems used so far. Although there will be pronounced quantitative inequalities, all actors are subject to the same playing field, unlike in the legal-state system, where some actors have qualitatively superior power because they control the rules themselves.

I believe that the role of Bitcoin is not only economic but also political and, therefore, deeply social. Following Bourdieu:

> What is at stake in the struggles about the meaning of the social world is power over the classificatory schemes and systems which are the basis of the representations of the groups and therefore of their mobilization and demobilization: the evocative power of an utterance which puts things in a different light (…) or which modifies the schemes of perception, shows something else, other properties, previously unnoticed or relegated to the background (…); a separative power, a distinction, *diacrisis*, *discretio*, drawing discrete units out of indivisible continuity, difference out of the undifferentiated.[3]

In this sense, Bitcoin and the blockchain are inventions that serve as tools in a struggle to redefine social relations. They use money, so to speak, as an excuse and as a basis for the possibility of non-hierarchical

[2] Ibid., 487–88.

[3] P. Bourdieu, "The Classification Struggle," In Distinction: A Social Critique of the Judgement of Taste (Harvard University Press, 1984).

social organization. The P2P management of economic transactions and trustless contracts, although still in its early stages, is already challenging a power hitherto perceived as necessary, and it already allows us to envision a future social organization that dispenses with it.

◆ A Social Theory of Cryptocurrencies

The social aspects of money are of interest, not to account for its origin, but for its role and function in a society.[4]

> The monetary system must be regarded as the fundamental factor responsible for providing the driving power stimulating the economic activities of all human society, except in a completely planned totalitarian system.[5]

Such a conclusion is consistent with Moini's definition of money: "*Money is a general claim against the stream of customary goods and services of a community.*"[6] In addition, monetary systems "provide their respective communities (...) with a stimulus for a higher degree of utilization of their productive faculties."[7] Throughout this second part, I have provided an account of how blockchain or distributed ledger technology addresses the recording of this right and thus constitutes a novel monetary instrument. On the one hand, the system's governing rules are public, both in their enunciation and in their application; on the other hand, the payment community is not restricted geographically or politically, but by voluntary association (even though different social environments provide various incentives to participate in this payment community).

A social theory of cryptocurrencies should be part of economic science, understood as a social science, which is problematic. On the one hand, social science gives little place to economics and the study of currency. The fact that half of this thesis is devoted to an account of theories about currency, both in economics and social sciences, and of empirical research on monetary systems, is exclusively due to the marginal position that the subject has in these sciences. On the other hand, most work in economics

[4] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 489.
[5] Ibid.
[6] Moini "Toward a General Theory of Credit and Money," 300.
[7] Einzig, Primitive Money in its Ethnological, Historical and Economic Aspects, 489.

denies the social character of this science and refuses to question or reflect on its fundamental concepts. This is what Moini calls *mathematicalism*:

> …that tendency within the post-1940's economic literature which assumes, usually tacitly, that "if it cannot be said with mathematics, then it cannot be economics." This is yet another of the manifestations of the preposterous methodology of positivism, adoption of which has done such great damage to the theoretical development of economics.[8]

To the already arduous task of tackling two fields of knowledge that are so far apart, we can add a third: computer science, which is essential for understanding the phenomenon of cryptocurrencies. As I anticipated in the introduction, most studies on cryptocurrencies are conducted from either a technical perspective, computer science, or formal neoclassical economics. Attempts to approach it from a humanistic perspective have been done from the (mostly Western or European) history of money, not going much further than establishing a time series of developments and projecting the future of that time series after the emergence of Bitcoin, as a new turning point.

This paper aims to fill that gap, approaching the phenomenon of cryptocurrencies from an anthropological perspective, considering both their technical aspects and the economic perspective. There are several important reasons why this work was relegated almost exclusively to the theoretical aspect. Future work in this area should delve deeper into the empirical social study of this phenomenon.

◆ Money and Civilization

Einzig raised the question of progress, or social transformations, and the relationship it may have with the evolution of money and currency:

> These criticisms lead us to the broader question whether the evolution of money in general over the whole period of its existence corresponded to contemporary requirements of civilization. The conflict lies between the school of thought which, on the basis of 19th-century prosperity and stability, maintains that the monetary system, under *laisser faire*, is bound to make for progress, and the

[8] Moini, "Toward a General Theory of Credit and Money," 314.

> opposite school which denounces the monetary system as the root of most if not all of the difficulties man has had to face throughout his long existence.
>
> There is also the more fundamental controversy between the school which maintains that the monetary system has throughout history been a decisive factor for good or evil, and has had a decisive influence on economic, political, social and cultural progress, and the opposite school which holds the views that, so far from being the cause of change, the monetary system has been throughout its history merely the effect of changes in the economic, political, social and cultural background.[9]

Perhaps today anthropology and the rest of the social sciences do not address these issues in these single cause-and-effect terms, but this question is of some interest if posed differently: what influence does the monetary system have on the rest of social institutions; or how well does the monetary system adapt to the transformation of other social relationships? Einzig finds further evidence to argue that not only does the money system have little influence on social change, but also that it tends to remain the same despite changes in social conditions:

> The difficulty is that the evolution of money and that of civilization are so closely interwoven that it is seldom possible to ascertain with any degree of assurance which was the cause and which the effect. Nevertheless, there are some clear instances in which progress in the monetary system lagged behind that of civilization.[10]
>
> ...money as a social factor has played an important part in all ages, not necessarily as an active factor making for the progress of civilization, but as a factor corresponding to the requirements of its own period and its own environment.[11]

It can be asserted that currency has a conservative character: Many commodity currencies remained in use for a long time even though society had been absorbed by global capitalism; even within industrial societies, the gold standard, for example, remained in use until the 1970s; and well into the 20th century and the digital age, the financial and banking system remained the same despite techno-scientific progress.

[9] Einzig, Primitive Money in its Ethnological, Historical and Economic Aspects, 500.
[10] Ibid., 500–01.
[11] Ibid., 504

Cryptocurrencies appeared more than a decade ago, and the narrative driving them is that they will bring social and political change. But, in retrospect, cryptocurrencies are the practical application of much older ideas.[12] The cypherpunk movement envisioned various technologies and software to bring about social transformation, not just digital money. This was clear to Nakamoto:

> Yes, [I will not find a solution to the political problems in cryptography,] but we can win a major battle in the arms race and gain a new territory of freedom for several years.
>
> Governments are good at cutting off the heads of a centrally controlled networks [sic] like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.[13]

◆ Change from Legal Tender to Cryptocurrency

To study why money has such a conservative character would require a whole body of research. In this brief chapter, I will take a moment to reflect on some of the considerations that come into play when the phenomenon of substituting one currency for another occurs, including both the obstacles and the easing.

In the case of the transition from commodity currency to legal tender, as described by Einzig, the main driving force behind the process was the political coercion of the colonial powers, rather than the internal economic dynamics of those traditional monetary systems. In my case, it is essential to differentiate between digital currency and cryptocurrency clearly. The digitization of payment methods is a process that began to emerge some time ago, with the introduction of credit cards. Cryptocurrencies, conversely, are characterized by their autonomy, i.e., the network manages their entire operation; their internal workings and robustness are built on cryptography, hence their name. This clarification is necessary to avoid confusion between two similar trends: on the one hand, the efforts of nation-states to eliminate cash to have a greater control over transactions made in their currency,[14] sometimes even resorting to blockchain technol-

[12] As it was stated on the Origin chapter.

[13] Nakamoto Bitcoin: *A Peer-to-Peer Electronic Cash System*.

[14] See, for example, the case of India: Vrishti Beniwal, "Poco Éxito y Muchos Problemas para el Adiós al Dinero en Efectivo en la India," *Perfil*, (2018).

ogy itself.[15] On the other hand, there is the dispute between legal tender currencies (whether digital or not) and cryptocurrencies, independent of the monetary policies of any nation-state.

As I discussed in the chapters in Part II, cryptocurrencies, particularly Bitcoin, have specific niches in which they are most useful: international payments, online shopping, savings, large transactions, and anonymous payments. The properties of transportability, indestructibility, divisibility, and knowability stand out, while homogeneity and stability of value are presented as problematic.

Einzig draws attention to a psychological phenomenon of great significance in the replacement of one monetary system by another:

> The difficulties of substituting modern money for primitive money, considerable as they are, are moderate compared with the difficulties of adapting primitive mentality to the requirements called for by the operation of a modern monetary system once it is introduced. For the satisfactory use of money for the purposes which it is meant to serve depends not only on qualities inherent in the money itself but also on the attitude of its users towards it.[16]

In this sense, I can speak not of primitive and modern mentalities, but of de jure and *de facto* mentalities, which seem to me to be more appropriate. The *de jure* mentality is that of an individual accustomed to the functioning of his or her economy within legal frameworks: a central bank that prints the currency with a backing, a banking system that manages the financial activities of its customers, and a justice system that protects everyone's private property. Cryptocurrencies operate *de facto*: one participates voluntarily, and depending on technical expertise, there is no backing, guarantors, or guarantees. The care of the property (i.e., the private keys) depends on the individual. However, there are many "bridges" between one world and the other (escrow services, legal regulatory frameworks, etc.), which introduce cryptocurrencies to various users without requiring a significant mental effort to learn about them and adapt one's mindset. The effect this may have, in the end, is to result in a monetary system that appears identical to legal tender, but which operates entirely in the background using Bitcoin or another cryptocurrency. I am not sure whether that is desirable, which is a subjective matter. Still, I certainly

[15] Javier Pastor, "China Prepara su Criptomoneda Digital Oficial, Llamada DC/EP, y Cuatro de sus Bancos ya Están Probándola en Móviles," *Xataka*, (2020).

[16] Einzig, *Primitive Money in its Ethnological, Historical and Economic Aspects*, 507.

think it is more likely to happen than a large contingent of people shifting from a *de jure* to a *de facto* mentality in a short period. The latter could, however, result from a generational change or another major crisis in the legal monetary system.

◆ The Future of Cryptocurrency

> I would be surprised if 10 years from now we're not using electronic currency in some way, now that we know a way to do it that won't inevitably get dumbed down when the trusted third party gets cold feet.
>
> — Satoshi Nakamoto, 2009.[17]

Ten years after he wrote those words, we indeed use electronic currency in various ways, and Bitcoin remains at the forefront of this, despite the huge proliferation of by-products derived from its source code. I do not want to predict what will happen in the next few years, but I would like to highlight some trends that I am certain will continue or intensify.

First, there is no longer any doubt that Bitcoin is not a passing thing, as might have been thought in its early years. Its usefulness is not only beginning to be perceived by major economic players but is also increasing with the development of its technology, organized in BIPs (Bitcoin Improvement Proposals). One of the main development focuses is the Lightning second layer,[18] a system for instant transactions of lesser amounts. Such a system would make Bitcoin viable as a small-scale medium of exchange by solving the problems discussed in the Economic (and Political) Role and Medium of Exchange chapters.

Second, a crack opens regarding the legality of Bitcoin: "regulators are seeking ways to monitor its use while, at the same time, more development and user effort is being pointed toward obscuring that use."[19] Today, large cryptocurrency exchanges and 'serious' cryptocurrency businesses require personal information from their users and are in contact with government authorities. Additionally, blockchain analytics companies analyze movements within the blockchain to identify the activity of these same users.

[17] S. Nakamoto, "Bitcoin v0.1 released," (2009).

[18] Joseph Poon and Thaddeus Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," (2016).

[19] Chawaga, Peter Chawaga, "As Analytics And Privacy Efforts Clash, Which Path Will Bitcoin Take?"

In that sense, these companies act as gateways between the legal tender and cryptocurrency economies, marking those who move from one side to the other and the coins that pass through them. The aim of these regulators is to closely monitor all economic activity and prevent 'dark money' from entering it. In the case of Bitcoin, accounts on these services have been flagged and frozen for being associated with addresses suspected of criminal activity and for using mixing services. In parallel, a large unregulated economy offers all the same services as the regulated one. The regulated crypto economy offers security in exchange for surrendering privacy, requiring a greater bureaucratic effort to comply with regulations, and exposing users to potential rejection. The deregulated economy, on the other hand, offers unrestricted and easy access in exchange for greater risk. A split is now emerging between the two, as the regulated economy rejects funds from the deregulated one. This rejection is not without reason, since with each new barrier put up by regulators, more users and capital are stepping aside.[20] Regulation can only be successful if it manages to keep the activity within its sphere of action, for which it must interfere discreetly or with a technical superiority that makes it impossible to escape its influence. On the other hand, a deregulated economy can be successful because it can effectively mitigate risk, i.e., prevent fraud and educate users so that they can operate autonomously and do not need to rely on third parties.

Third. As can be seen, especially in the chapters on altcoins, cryptocurrencies, as a public technology and a common good, offer the opportunity for any individual, business, or community to create a monetary system tailored to their specific needs. A bit like Hayek's "Denationalization of money," but without even needing banks to manage them. Cryptocurrencies and blockchains represent another iteration in the development of peer-to-peer (P2P) relationships. Like other technologies of this type, it is exceedingly difficult for them to disappear once they are established. Cryptocurrencies and blockchains are highly versatile technologies whose applications are just beginning to emerge.

This brings me to the fourth point. In the not-too-distant future, Bitcoin, cryptocurrencies in general, or blockchain technology could cease to participate in the contest between currencies and become the arena where

[20] Rick D., "Usuarios Retiran $200 Millones de Coinbase tras Acuerdo con el Gobierno de EE. UU." *BeInCrypto*, (2020).

disputes occur. That is, as I mentioned in the previous chapter, Bitcoin could become the back end, the hidden infrastructure that underlies the global financial system, presented under another guise, or the international standard. Or, in any case, it might not be Bitcoin the network, but the blockchain technology that does this, as it is a long-standing trend among the establishment to separate the blockchain from Bitcoin. Some countries, such as China and Venezuela, have already implemented their own national cryptocurrency; the United States does not want to be left behind in this race.[21] Instead of creating their own cryptocurrency, other internationally sanctioned countries, such as Cuba,[22] Korea,[23] and Iran, turn to Bitcoin.[24] The case for Bitcoin to become the international standard may stem from distrust between governments. International policy analysts have discussed the "end of globalization" since at least the 2008 crisis.[25] The end of globalization primarily implies the end of US hegemony in geopolitics and economics. This, in turn, means abandoning the dollar standard in international trade. The chances of another power taking its place are not high, or at least not in the immediate future. This is why one power cannot unilaterally dictate the international standard; a power vacuum could introduce Bitcoin as a Trojan horse in international trade. However, other powers could introduce their own currencies within their spheres of influence, resulting in a multipolar scenario where different regions each have their own individual currency, and Bitcoin, apart from being a currency of its own, serves as a currency for everyone and no one.

[21]Tatiana Koffman, "U.S. Moves Closer To Digital Dollar," Forbes (2020).

[22]elEconomista.es, "Cuba Estudia el uso de Criptomonedas para Impulsar su Economía ante las Sanciones de Estados Unidos," (2019).

[23]Yuji Nakamura, "North Korea Hackers Step Up Bitcoin Attacks," Bloomberg.com (2017).

[24]Tanvi Ratna, "Iran Has a Bitcoin Strategy to Beat Trump," Foreign Policy, (2020).

[25]Paul Smith, "Flowback or the End of Globalization," IIM Kozhikode Society & Management Review 3, no.1 (2014), 1-9.

Sources

Adams, Hayden (2018). *Uniswap Whitepaper*. Accessed 19 July 2021. URL: https://hackmd.io/@HaydenAdams/HJ9jLsfTz#%F0%9F%A6%84-Uniswap-Whitepaper.

Addessi, Elsa et al. (2011). "How Social Context, Token Value, and Time Course Affect Token Exchange in Capuchin Monkeys (Cebus Apella)". In: *International Journal of Primatology* 32.1, pp. 83–98. DOI: 10.1007/s10764-010-9440-4.

Albrecht, Radoslav (Aug. 2013). "Bitcoin Volatility - The 4 Perspectives". In: *Bitcoin Magazine*. URL: https://bitcoinmagazine.com/articles/bitcoin-volatility-analysis-1377627247.

Alizart, Mark (2020). *Cryptocommunism. Theory Redux*. Polity Press. URL: https://libgen.rs/book/index.php?md5=A666241D7F49D33F423E5AE1776D19EA.

Ammous, Saifedean (2018). *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. 1st. Wiley. URL: https://libgen.rs/book/index.php?md5=7D394651158ABC9470CBCCE538FAAA49.

Amusing Planet (2014). *Rai Stones from Yap*. URL: https://www.amusingplanet.com/2014/06/the-giant-stone-coins-of-yap.html.

Ancient History Encyclopedia Foundation (n.d.). *Writing Timeline*. https://www.ancient.eu/timeline/writing/.

Antiporovich, Nicolás (2020a). "DeFi Madness: One Person Earned 16,000 USDC in 13 Seconds with a Flash Loan". In: *CriptoNoticias - Bitcoin, Blockchains and Cryptocurrencies* 5. URL: https://www.criptonoticias.com/mercados/defi-persona-gano-usdc-segundos-prestamo-flash-loan/.

— (Aug. 22, 2020b). "Rodolfo Andrages, el Argentino que Registró el Dominio Bitcoins.com en el Año 2000". In: *CriptoNoticias - Bitcoin, Blockchains y Criptomonedas*. Accessed 31 August 2020. URL: https:

//www.criptonoticias.com/comunidad/adopcion/rodolfo-andranges-bitcoin-eficiente-gente-crea-en-el/.

Antonopoulos, Andreas (2017). *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media. URL: https://github.com/bitcoinbook/bitcoinbook/blob/develop/book.asciidoc.

Aristotle (2004). *Nicomachean Ethics*. 2nd. Cambridge Texts in the History of Philosophy. Cambridge, UK: Cambridge University Press. URL: https://libgen.rs/book/index.php?md5=5713D150505DAD1B2D8150D2C2F809ED.

Armstrong, W. E. (1924). "Rossel Island Money: A Unique Monetary System". In: *The Economic Journal* 34.135, pp. 423–429. DOI: 10.2307/2222650.

Back, Adam (Mar. 1997). *[ANNOUNCE] Hash Cash Postage Implementation*. URL: http://www.hashcash.org/papers/announce.txt.

— (2002). *Hashcash - A Denial of Service Counter-Measure*. URL: http://www.hashcash.org/papers/hashcash.pdf.

Barlow, John Perry (1996). *A Declaration of the Independence of Cyberspace*. https://www.eff.org/cyberspace-independence.

Beam Foundation (2020). *Beam Position Paper*. URL: https://docs.beam.mw/BEAM_Position_Paper_0.3.pdf.

Ben-Sasson, Eli et al. (2014). "Zerocash: Decentralized anonymous payments from bitcoin". In: *IEEE Symposium on Security and Privacy*. IEEE, pp. 459–474. URL: http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf.

Bendiksen, Christopher and Samuel Gibbons (2018). *The Bitcoin Mining Network: Trends, Composition, Marginal Creation Cost, Electricity Consumption & Sources MAY 2018 UPDATE*. Tech. rep. Coinshares Research. URL: https://coinsharesgroup.com/assets/resources/Research/bitcoin-mining-network-may-2018.pdf.

Bendiksen, Christopher, Samuel Gibbons, and Eugene Lim (2018). *The Bitcoin Mining Network: Trends, Composition, Marginal Creation Cost, Electricity Consumption & Sources NOVEMBER 2018 UPDATE*. Tech. rep. Coinshares Research & Three Body Capital. URL: https://coinsharesgroup.com/assets/resources/Research/bitcoin-mining-network-november-2018.pdf.

Beniwal, Vrishti (Sept. 24, 2018). "Poco Éxito y Muchos Problemas para el Adiós al Dinero en Efectivo en la India". In: *Perfil*. Accessed 22 August

2020. URL: https://www.perfil.com/bloomberg/bc-poco-exito-y-muchos-problemas-para-la-desmonetizacion-de-india.phtml.

Bernholz, Peter (2003). *Monetary Regimes and Inflation: History, Economic and Political Relationships*. Edward Elgar Publishing. URL: https://libgen.rs/book/index.php?md5=84105F8CA308B24C865B9CA3885E8347.

Bianconi, G. and A.-L. Barabási (2001). "Competition and Multiscaling in Evolving Networks". In: *Europhysics Letters* 54.5, pp. 436–442. DOI: 10.1209/epl/i2001-00260-6.

Bitcoin Magazine (n.d.). *What Are Bitcoin Mixers*. URL: https://bitcoinmagazine.com/guides/what-are-bitcoin-mixers.

Bitcoin Wiki (n.d.[a]). *Block Hashing Algorithm*. URL: https://en.bitcoin.it/wiki/Block_hashing_algorithm.

— (n.d.[b]). *Block Size Limit Controversy*. URL: https://bitcoinwiki.org/wiki/block-size-limit-controversy.

— (n.d.[c]). *Difficulty*. URL: https://en.bitcoin.it/wiki/Difficulty.

— (n.d.[d]). *OP Return*. URL: https://en.bitcoin.it/wiki/OP_RETURN.

— (n.d.[e]). *Private Key*. URL: https://en.bitcoin.it/wiki/Private_key.

— (n.d.[f]). *Script*. URL: https://en.bitcoin.it/wiki/Script.

Bitcoin.org (n.d.). *Wallet*. URL: https://bitcoin.org/en/vocabulary%5C#wallet.

BitShares Blockchain Foundation (2019). *BitShares Documentation*. Accessed 1 August 2020. URL: https://how.bitshares.works/en/master.

Blockchain.com (n.d.). *Average Block Size*. URL: https://www.blockchain.com/explorer/charts/avg-block-size?timespan=all.

Borges, Jorge Luis (1949). "El Zahir". In: *El Aleph*. Buenos Aires: Editorial Losada, pp. 73–82.

Bourdieu, Pierre (1984). *Distinction: A Social Critique of the Judgement of Taste*. Harvard University Press. URL: https://libgen.rs/book/index.php?md5=65DB191C595A7E9234368D879AE4D156.

Buterin, Vitalik (2013). *A Next-Generation Smart Contract and Decentralized Application Platform*. URL: https://ethereum.org/en/whitepaper/.

Carjuzaa, Maximiliano, Alejandro Bokser, and Javier García Sánchez (2019). *Money On Chain: Protocolo de una Stablecoin Colateralizada con Bitcoin*. URL: https://drive.google.com/file/d/1GYJaNpNnfI4L2LT3yTHQhtKfSILVRvGE/view.

Casey, Michael J. (May 21, 2018). "Crypto Tribalism Is Holding Back Blockchain". In: *Coindesk*. URL: https://www.coindesk.com/crypto-tribalism-holding-back-blockchain.

Chainalysis Team (2018). *Bitcoin Investors and Speculators Hold Their Positions over the Summer*. URL: https://blog.chainalysis.com/reports/money-supply-q3.

Champagne, Phil (2014). *The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto*. e53 Publishing, LLC. URL: https://www.bookofsatoshi.com/.

Chaum, David (1983). "Blind Signatures for Untraceable Payments". In: *Advances in Cryptology*. DOI: 10.1007/978-1-4757-0602-4_18.

Chawaga, Peter (Nov. 7, 2019). "BTC Bullion: Three Interpretations of Bitcoin as "Digital Gold"". In: *Bitcoin Magazine*. URL: https://bitcoinmagazine.com/articles/bitcoin-as-digital-gold.

— (July 16, 2020). "As Analytics And Privacy Efforts Clash, Which Path Will Bitcoin Take?" In: *Bitcoin Magazine*. URL: https://bitcoinmagazine.com/articles/as-analytics-and-privacy-efforts-clash-which-path-will-bitcoin-take.

Chayanov, A. V. (1966). *The Theory of Peasant Economy*. Translation Series. Richard D. Irwin. URL: https://libgen.rs/book/index.php?md5=967720F869237F5B893AE518B3477C6C.

Clarín (Sept. 3, 2002). *Denuncian un Complot para Destruir el Sistema del Trueque*. URL: https://www.clarin.com/sociedad/denuncian-complot-destruir-sistema-trueque%5C_0%5C_B1tgKWNIAFl.html.

CME Group (n.d.). *Bitcoin Futures and Options*. URL: https://www.cmegroup.com/markets/cryptocurrencies/bitcoin/bitcoin.contractSpecs.html.

Coase, R. H. (1937). "The Nature of the Firm". In: *Economica*. New Series 4.16, pp. 386–405. DOI: 10.1111/j.1468-0335.1937.tb00002.x.

Colmenares, José (July 31, 2020). "Putin Firmó ley que Prohíbe Pagos con Bitcoin y Criptomonedas en Rusia". In: *CriptoNoticias - Bitcoin, Blockchains y Criptomonedas*. URL: https://www.criptonoticias.com/gobierno/regulacion/putin-firmo-ley-prohibe-pagos-bitcoin-criptomonedas-rusia.

Conye, Christopher J. and Abigail R. Hall (2017). *Four Decades and Counting. The Continued Failure of the War on Drugs*. Tech. rep. Cato Institute.

Cuen, Leigh (Aug. 22, 2019). "In Palestine, Civilians Are Using Bitcoin More Than Hamas". In: *Coindesk*. URL: https://www.coindesk.com/palestinian-civilians-are-using-bitcoin-more-than-terrorists.

Dahlman, Carl J. (1979). "The Problem of Externality". In: *The Journal of Law and Economics* 22.1, pp. 141–162. DOI: 10.1086/466936.

Dai, Wei (1998). *B-Money*. URL: https://nakamotoinstitute.org/b-money/.

Darwin, Charles (1859). *On the Origin of Species by Means of Natural Selection, or Preservation of Favored Races in the Struggle for Life*. John Murray.

De, Nikhilesh, Stan Higgins, and Muyao Shen (Aug. 22, 2018). "SEC Rejects 9 Bitcoin ETF Proposals". In: *Coindesk*. URL: https://www.coindesk.com/markets/2018/08/22/sec-rejects-9-bitcoin-etf-proposals.

Denninger, Karl (Mar. 30, 2013). *BitCon: Don't*. URL: http://market-ticker.org/akcs-www?post=219284.

Dian, Mario (n.d.). *Cost of a 51% Attack and Security of Bitcoin, Monero, Litecoin and Other Cryptocurrencies*. URL: https://freedomnode.com/blog/86/cost-of-51-attack-and-security-of-bitcoin-monero-litecoin-and-other-cryptocurrencies.

Díaz, Genny (2019). "Apagones en Venezuela Revelan Uso de Bitcoin para Envío de Remesas en Latinoamérica". In: *Criptonoticias*.

DiCamillo, Nathan (June 12, 2020). "This Liechtenstein Bank Can Now Custody Crypto". In: *Coindesk*. URL: https://www.coindesk.com/this-liechtenstein-bank-can-now-custody-crypto.

Dingledine, Roger, Nick Mathewson, and Paul Syverson (Jan. 1, 2004). *Tor: The Second-Generation Onion Router*. Tech. rep. Defense Technical Information Center. URL: https://doi.org/10.21236/ADA465464.

Duran, Enric, Thomas König, and Roland Alton Niklas Fessler (2018). *The Proof-of-Cooperation Blockchain FairCoin*. URL: https://fair-coin.org/sites/defaul%20t/files/FairCoin2_whitepaper%5C_V1.2.pdf.

Durkheim, Émile (1915). *The Elementary Forms of the Religious Life, a Study in Religious Sociology*. G. Allen & Unwin LTD. URL: https://archive.org/details/elementaryformso00durkrich.

— (2017). *The Division Of Labour In Society*. Collier-Macmillan Limited. URL: https://archive.org/details/in.ernet.dli.2015.126617.

Ebay (n.d.). *Seashell coin necklace presumably ancient and from New Guinea*. URL: https://www.ebay.co.uk/itm/Antique-old-Papua-New-Guinea-conus-shell-money-currency-necklace-65-cm-/252014118389.

Einzig, Paul (1966). *Primitive Money in its Ethnological, Historical and Economic Aspects*. Eyre & Spottiswoode.

elEconomista.es (July 3, 2019). "Cuba Estudia el uso de Criptomonedas para Impulsar su Economía ante las Sanciones de Estados Unidos". In: Accessed 24 August 2020. URL: https://www.eleconomista.es/economia/noticias/9973970/07/19/Cuba-estudia-el-uso-de-criptomonedas-para-impulsar-su-economia-ante-las-sanciones-de-EEUU.html.

Electric Capital (2019). *Electric Capital Developer Report (H1 2019)*. URL: https://medium.com/electric-capital/electric-capital-developer-report-h1-2019-7d836d68fecb.

Elliott, Francis and Gary Duncan (Jan. 3, 2009). "Chancellor Alistair Darling on Brink of Second Bailout for Banks". In: *The Times*. URL: https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h.

Wu-emma (n.d.). *Bitgesell*. URL: https://bitgesell.ca/.

Engels, Friedrich (2021). *The Origin of the Family, Private Property and the State*. Marxists Internet Archive. URL: https://www.marxists.org/archive/marx/works/1884/origin-family/index.htm.

Esparragoza, Luis (Feb. 14, 2017). "Mineros Venezolanos Apagan sus Equipos por Temor a Persecución Policial". In: *Criptonoticias*. URL: https://www.criptonoticias.com/comunidad/mineros-venezolanos-apagan-equipos-temor-persecucion-policial/.

Euler, Leonhard (1741). "Solutio Problematis ad Geometriam Situs Pertinentis". In: *Commentarii Academiae Scientiarum Petropolitanae* 8.

Fanti, Giulia et al. (2018). "Dandelion++: Lightweight Cryptocurrency Networking With Formal Anonymity Guarantees". In: *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 2.2, pp. 1–35. DOI: 10.1145/3224424.

Faria, Emily (2021). "Bitcoin Energy Consumption Debunked". In: *Bitrawr*. URL: https://www.bitrawr.com/mining/bitcoin-energy-consumption-debunked.

Finney, Hal (1993). *Detecting Double Spending*. URL: https://nakamotoinstitute.org/detecting-double-spending/.

Fisher, Irving (1933). "The Debt-Deflation Theory of Great Depressions". In: *Econometrica* 1.4, pp. 337–357. DOI: 10.2307/1907327.

Forma de gobierno (n.d.). Accessed 1 August 2020. URL: https://monedapar.com.ar/forma-de-gobierno.

Foundation, Wikimedia (n.d.[a]). *Bitcoin Scalability Problem*. URL: https://en.wikipedia.org/wiki/Bitcoin_scalability_problem.

— (n.d.[b]). *Chomsky Hierarchy*. URL: https://en.wikipedia.org/wiki/Chomsky_hierarchy.

— (n.d.[c]). *Knut Wicksell*. URL: https://en.wikipedia.org/wiki/Knut_Wicksell.

— (n.d.[d]). *Silk Road (Marketplace)*. URL: https://en.wikipedia.org/wiki/Silk_Road_(marketplace).

— (n.d.[e]). *WannaCry Ransomware Attack*. URL: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.

Frankenfield, Jake (2019). *Hodl*. URL: https://www.investopedia.com/terms/h/hodl.asp.

Franklin, Benjamin (1961). "Advice to a Young Tradesman". In: *The Papers of Benjamin Franklin*. Ed. by Leonard W. Labaree. Vol. 3. Accessed through Founders Online, National Archives. New Haven: Yale University Press, pp. 304–308. URL: https://founders.archives.gov/documents/Franklin/01-03-02-0130.

Fred, Alexander (Feb. 27, 2019). "What Does "1 BTC = 1 BTC" Even Mean?" In: *Be[in]Crypto*. URL: https://beincrypto.com/what-does-1-btc-1-btc-even-mean.

Friedenbach, Mark and Jorge Timón (2015). *Freicoin*. URL: http://freico.in/.

Friedman, Milton and Anna J. Schwartz (1963). "Money and Business Cycles". In: *Review of Economics and Statistics* 45.1. DOI: 10.2307/1927148.

Funcionamiento del Sistema (n.d.). Accessed 1 August 2020. URL: https://monedapar.com.ar/funcionamiento-del-sistema.

Fundamentos Monetarios (n.d.). Accessed 1 August 2020. URL: https://monedapar.com.ar/fundamentos-monetarios.

Gadamer, Hans-Georg (2013). *Truth and Method*. 3rd. Bloomsbury Revelations. Bloomsbury Academic. URL: https://libgen.rs/book/index.php?md5=06D87BCE24D3B07D4479F1872520EDD5.

Galt, Juan (Dec. 22, 2015). *Is Bitcoin Headed for a Break in Fungibility?* URL: https://bitcoinmagazine.com/articles/is-bitcoin-headed-for-a-break-in-fungibility-1450823559.

García-Siñeriz, M. Peyrouzet (2018). "In Blockchain They Trust - Now, Power to the People or to the Invisible Hand: An Analysis of the Ideological Tensions and Affinities Between Crypto-libertarian and Crypto-commonist Visions, Projects and Aspirations for the Blockchain Revolution". PhD thesis. University of Exeter. URL: https://www.academia.edu/38081197/In_blockchain_they_trust_-_Now_power_to_the_people_or_to_the_invisible_hand.

Geier, Maximiliano Iván (2018). "Análisis del Comportamiento de Aplicaciones Paralelas y Distribuidas por Medio de Técnicas de Emulación de Redes". PhD thesis. Universidad de Buenos Aires. URL: https://bibliotecadigital.exactas.uba.ar/download/tesis/tesis_n6538_Geier.pdf.

Gesell, Silvio (1958). *The Natural Economic Order*. Peter Owen Ltd. URL: https://www.silvio-gesell.de/the-natural-economic-order.html.

Giffen, Robert (1891). "The Gresham Law". In: *The Economic Journal* 1.2. DOI: 10.2307/2956251.

GoBitcoin.io (n.d.). *Cost of a 51% Attack*. URL: https://gobitcoin.io/tools/cost-51-attack/.

Godelier, Maurice (1969). "La 'Monnaie de Sel' des Baruya de Nouvelle-Guinée". In: *L'Homme* 9.2, pp. 5–37. DOI: 10.3406/hom.1969.367046.

— (1971). ""Salt Currency" and the Circulation of Commodities among the Baruya of New Guinea". In: *Studies in Economic Anthropology*. American Anthropological Association. URL: https://archive.org/details/studiesineconomi00dalt/page/2/mode/2up.

— (1974). *Economía, Fetichismo y Religión en las Sociedades Primitivas*. Siglo.

— (1987). *The Making of Great Men: Male Domination and Power among the New Guinea Baruya*. Press Syndicate of the University of Cambridge. URL: https://archive.org/details/makingofgreatmen0000godea/mode/2up.

Gómez, Georgina M. (2009). *Argentina's Parallel Currency: The Economy of the Poor*. Picketing & Chatto Ltd. URL: https://libgen.rs/book/index.php?md5=2C90663784B97037AB38B04BB1896945.

Gómez, Iván (Mar. 28, 2020). "Bitcoin Contra el Autoritarismo: Caso Venezuela". In: *Criptonoticias*. URL: https://www.criptonoticias.com/opinion/bitcoin-contra-autoritarismo-caso-venezuela.

Goonsack (2013). *What a Landmark Legal Case from Mid-1700s Scotland Tells Us about the Fungibility and the Very Nature of Money– and Why We Should Care in Light of the Recent CoinValidation Controversy*. URL: https://www.reddit.com/r/Bitcoin/comments/1qomqt/what_a_landmark_legal_case_from_mid1700s_scotland.

Graeber, David (2004). *Fragments of an Anarchist Anthropology*. Prickly Paradigm Press. URL: https://libgen.rs/book/index.php?md5=CD15C238F495257A4199AE655E3C192C.

— (2011). *Debt: The First 5000 Years*. Melville House Publishing. URL: https://libgen.rs/book/index.php?md5=784A4D178F690858F66331408070A498.

Griffin, John M. and Amin Shams (2019). "Is Bitcoin Really Un-Tethered?" In: *Social Science Research Network*. DOI: 10.2139/ssrn.3195066.

Hammill, Chuck (1987). *From Crossbows To Cryptography: Techno-Thwarting The State*. URL: https://nakamotoinstitute.org/static/docs/from-crossbows-to-cryptography.pdf.

Hammurabi, King of Babylon (2011). *The Code of Hammurabi*. URL: http://www.general-intelligence.com/library/hr.pdf.

Harper, Colin (Mar. 28, 2019). "Innisfil Becomes First City in Canada to Accept Bitcoin for Municipal Taxes". In: *Bitcoin Magazine*. URL: https://bitcoinmagazine.com/articles/innisfil-becomes-first-city-canada-accept-bitcoin-municipal-taxes.

Hayek, Friedrich A. (1990). *Denationalization of Money, An Analysis of the Theory and Practice of Concurrent Currencies*. Coronet Books. URL: https://libgen.rs/book/index.php?md5=00703D16505793E59E832EFB40D168FC.

Hearn, Mike (2013). *Re: Could Satoshi Come Back and Tell Us What He/Her Thinks about the Block Size?* URL: https://bitcointalk.org/index.php?topic=145850.msg1558053%5C#msg1558053.

Hesiod (1914). *Works and Days*. Trans. by Hugh G. Evelyn-White. Florida State University. URL: https://people.sc.fsu.edu/~dduke/lectures/hesiod1.pdf.

Hilbert, David and Wilhelm Ackermann (1938). *Grundzüge der Theoretischen Logik*. 2nd. Vol. 27. Die Grundlehren der mathe-

matischen Wissenschaften in Einzeldarstellungen. Julius Springer. URL: https://libgen.rs/book/index.php?md5=9B1FEAA5870AD46F25B25EA4CA5A88CC.

Hildebrand, Bruno (1864). "Naturalwirthschaft, Geldwirthschaft und Creditwirthschaft". In: 2, pp. 1–24. DOI: 10.2307/23840074.

Hill, Kashmir (Nov. 13, 2013). "Sanitizing Bitcoin: This Company Wants To Track "Clean" Bitcoin Accounts". In: *Forbes*. URL: https://www.forbes.com/sites/kashmirhill/2013/11/13/sanitizing-bitcoin-coin-validation.

Hirota, Yasuyuki (2017). "Monedas sociales y complementarias (MSCs): Sus valores socioeconómicos para distintos stakeholders". PhD thesis. Institut Universitari d'Investigació en Economia Social, Cooperativisme i Emprenedoria (IUDESCOOP). URL: http://roderic.uv.es/bitstream/handle/10550/60937/Tesis%20doctoral.pdf.

Hoenicke, Jochen (n.d.). *Johoe's Bitcoin Mempool Size Statistics*. URL: https://jochen-hoenicke.de.

Hughes, Eric (Mar. 9, 1993). *A Cypherpunk's Manifesto*. URL: https://www.activism.net/cypherpunk/manifesto.html.

Hunt, Mary Ebbets (n.d.). *Chilkat blanket*. https://en.wikipedia.org/wiki/Chilkat_weaving#/media/File:Mary_Ebbets_Hunt_-_Chilkat_blanket.jpg.

I2P: Un Sistema Escalable para las Comunicaciones Anónimas (n.d.). URL: https://geti2p.net/es/docs/how/tech-intro.

Ibarra, Juan (Jan. 9, 2020). "Informe: Bitcoin Seguirá Ganando en Adopción Sobre otras Criptomonedas en 2020". In: *Criptonoticias*. URL: https://www.criptonoticias.com/comunidad/adopcion/informe-bitcoin-ganando-adopcion-otras-criptomonedas-2020.

Jablonko, Allison, Marek Jablonko, and Maurice Godelier (2011). *Study Guide for the Films TO FIND THE BARUYA STORY and HER NAME CAME ON ARROWS*. Accessed 31 August 2020. URL: https://jablonko-baruya.pacific-credo.fr/.

Jedusor, Tom Elvis (2016). *Mimblewimble*. URL: https://scalingbitcoin.org/papers/mimblewimble.txt.

Jevons, William Stanley (1877). *Money and the Mechanism of Exchange*. D. Appleton and Company. URL: https://archive.org/details/cu31924031196623/page/n5/mode/2up.

Jones, Noel (2013a). "Bitcoin, Bootstrapping, and the Black Market". In: *Bitcoin Theory*. URL: https://btheory.com/2013/08/09/bitcoin-bootstrapping-and-the-black-market.

— (2013b). "The Intrinsic Value of Bitcoin". In: *Bitcoin Theory*. URL: https://btheory.com/2013/09/10/what-is-bitcoins-intrinsic-value/.

— (2014a). "Bitcoin Is a Commodity Money". In: *Bitcoin Theory*. URL: https://btheory.com/2014/11/19/bitcoin-as-a-commodity-money/.

— (2014b). "Gresham's Law and Bitcoin". In: *Bitcoin Theory*. URL: https://btheory.com/2014/08/07/greshams-law-and-bitcoin/.

Keynes, John Maynard (1937). "The General Theory of Employment". In: *Quarterly Journal of Economics* 51.2, pp. 209–223. DOI: 10.2307/1882087.

— (1964). "Chapter 15: The Psychological and Business Incentives to Liquidity". In: *The General Theory of Employment, Interest and Money*. Harcourt Brace Jovanovich. URL: https://libgen.rs/book/index.php?md5=DD7CF488F45954B38061249E5F046B32.

— (2012a). "A Treatise on Money: The Applied Theory of Money". In: *The Collected Writings of John Maynard Keynes*. Vol. 6. Cambridge University Press. URL: https://libgen.rs/book/index.php?md5=26CD1CBAB5FC779CD4D2408C0028E5FB.

— (2012b). "A Treatise on Money: The Pure Theory of Money". In: *The Collected Writings of John Maynard Keynes*. Vol. 5. Cambridge University Press. URL: https://libgen.rs/book/index.php?md5=E163207BF71BA2EE64632DBC19F09E90.

King, Sunny and Scott Nadal (2012). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. URL: https://www.peercoin.net/whitepapers/peercoin-paper.pdf.

Knapp, Georg Friedrich (1924). *The State Theory of Money*. Macmillan & Company Limited. URL: https://socialsciences.mcmaster.ca/~econ/ugcm/3ll3/knapp/StateTheoryMoney.pdf.

Knizhnik, Konstantin (2008). "Patricia Tries: A Better Index For Prefix Searches". In: *Dr. Dobb's*. URL: https://www.drdobbs.com/architecture-and-design/patricia-tries/208800854.

Koffman, Tatiana (July 1, 2020). "U.S. Moves Closer To Digital Dollar". In: *Forbes*. Accessed 24 August 2020. URL: https://www.forbes.com/sites/tatianakoffman/2020/07/01/senate-moves-closer-to-digital-dollar/.

KYCNot.me (n.d.). *KYC-Free Crypto Freedom*. URL: https://kycnot.me/.

Ladeluca, John (July 21, 2020). "Best Bitcoin Bitcoin Debit and Credit Cards in 2020 – InsideBitcoins". In: *InsideBitcoins.com*. URL: https://insidebitcoins.com/bitcoin-debit-credit-cards.

Ladygina-Kohts, Nadezhda Nikolaevna (2002). *Infant Chimpanzee and Human Child: A Classic 1935 Comparative Study of Ape Emotions and Intelligence*. Oxford University Press. URL: https://books.google.com/books?id=6KN6GuoHPF4C&lpg=PP1&dq=Infant+chimpanzee+and+human+child:+A+classic+1935+comparative+study+of+ape+emotions+and+intelligence&pg=PP1.

Lamport, Leslie, Robert Shostak, and Marshall Pease (1981). *The Byzantine Generals Problem*. Tech. rep. SRI International. URL: https://nakamotoinstitute.org/static/docs/the-byzantine-generals-problem.pdf.

Laszlo (2010). *Pizza for Bitcoins?* Bitcoin Forum. URL: https://bitcointalk.org/index.php?topic=137.0.

Lerner, Sergio Demian (2019). *Rsk*.
textitRootstock Core Team, White Paper. URL: https://www.rsk.co/es/Whitepapers/RSK-White-Paper-Updated-es.pdf.

Levi, Primo (1959). *If This Is a Man*. The Orion Press. URL: https://libgen.rs/book/index.php?md5=88FD48C89CE756518D72BD9BCF2853E5.

— (2015). *The Complete Works of Primo Levi*. Liveright Publishing Corporation. URL: https://libgen.rs/book/index.php?md5=06F0B7188CE0B3476CD1FED825FE2EDC.

Lucchini, Lorenzo et al. (2020). *From Code to Market: Network of Developers And Correlated Returns of Cryptocurrencies*. Tech. rep. URL: https://arxiv.org/pdf/2004.07290.pdf.

Lukács, Georg (1971). "Reification and the Consciousness of the Proletariat, I. The Phenomenon of Reification". In: *History and Class Consciousness: Studies in Marxist Dialectics*. The Merlin Press Ltd. URL: https://libgen.rs/book/index.php?md5=4D539CEEF59B4CA85066027CE59C87DD.

Macleod, Henry Dunning (1891). *The Elements of Banking*. Longmans, Green and Co. URL: https://archive.org/details/in.ernet.dli.2015.22182/.

— (1893). *The Theory of Credit*. 2nd edn. Vol. 1. Longmans, Green and Co. URL: https://archive.org/details/theoryofcredit01macl_uoft/page/n8/mode/2up.

— (1894). *The Theory of Credit*. 2nd edn. Vol. 2. Longmans, Green and Co. URL: https://archive.org/details/p1theoryofcredit02macluoft/page/n6/mode/2up.

— (1897). *The Theory of Credit*. 2nd. Vol. 2 vols. Longmans, Green and Co. URL: https://archive.org/details/p2theoryofcredit02macluoft/page/n6/mode/2up.

Majamalu (July 2017). *Escenarios Posibles a Partir del Fork*. URL: https://elbitcoin.org/escenarios-posibles-partir-del-fork/.

Maker Foundation (2020). *The Maker Protocol White Paper*. Accessed 20 June 2022. URL: https://makerdao.com/en/whitepaper/.

Marx, Karl (1999). *A Contribution to the Critique of Political Economy*. Marxists Internet Archive. URL: https://www.marxists.org/archive/marx/works/download/Marx_Contribution_to_the_Critique_of_Political_Economy.pdf.

— (2015). *The Capital*. First English Edition. Vol. 1. Marxists Internet Archive. URL: https://www.marxists.org/archive/marx/works/download/pdf/Capital-Volume-I.pdf.

Matonis, Jon (2012). "Could Bitcoin Become the Currency of System D?" In: *Forbes*. URL: https://www.forbes.com/sites/jonmatonis/2012/03/19/could-bitcoin-become-the-currency-of-system-d.

Mauss, Marcel (1914). "Les Origines de la Notion de Monnaie". In: *Comptes-rendus des Séances* 1.2, pp. 14–19. DOI: 10.1522/CLA.MAM.ORI.

— (2002). *The Gift. The Form and Reason for Exchange in Archaic Societies*. Routledge Classics. URL: https://libgen.rs/book/index.php?md5=94CC57CD150CBAA241552B02E8FD76E9.

Maxwell, Gregory (2013). *Transaction Cut-Through*. Bitcoin Forum. URL: https://bitcointalk.org/index.php?topic=281848.0.

— (2015). *Confidential Values*. URL: https://web.archive.org/web/20191122230510/https://people.xiph.org/~greg/confidential_values.txt.

May, Timothy C. (Sept. 1992). *The Crypto Anarchist Manifesto*. URL: https://activism.net/cypherpunk/crypto-anarchy.html.

— (1994). *Crypto Anarchy and Virtual Communities*. URL: https://nakamotoinstitute.org/virtual-communities/.

Mempool Space (n.d.). https://mempool.space/.

Menger, Carl (1892). "On the Origin of Money". In: *The Economic Journal* 2.6, pp. 239–255. DOI: 10.2307/2956146.

— (2007). *Principles of Economics*. Ludwig von Mises Institute. URL: https://mises.org/library/principles-economics.

Meunier, Sebastien (Jan. 2018). "Can Bitcoin Be Destroyed? 7 (Unlikely) Paths to Irrelevance". In: *Coindesk*. URL: https://www.coindesk.com/can-bitcoin-be-destroyed-7-unlikely-paths-irrelevance.

Meyer, David (Sept. 2017). "This Place Lets You Pay Your Taxes In Bitcoin". In: *Fortune*. URL: https://fortune.com/2017/09/12/switzerland-chiasso-bitcoin-tax-zug.

Mises, Ludwig von (2009). *The Theory of Money and Credit*. Ludwig von Mises Institute. URL: https://mises.org/library/theory-money-and-credit.

Moini, Mostafa (2001). "Toward a General Theory of Credit and Money". In: *The Review of Austrian Economics* 14.4, pp. 267–317. DOI: 10.1023/A:1011933129866.

Monero (n.d.). *About Monero*. URL: https://web.getmonero.org/es/resources/about/.

Morgan, Lewis Henry (1982). *Ancient Society or Researches in the Lines of Human Progress from Savagery through Barbarism to Civilization*. Calcutta: K. P. Bagchi & Company. URL: https://archive.org/details/in.ernet.dli.2015.174214.

Morrison, Donald R. (1968). "PATRICIA—Practical Algorithm To Retrieve Information Coded in Alphanumeric". In: *Association for Computing Machinery* 15.4, pp. 514–534. DOI: 10.1145/321479.321481.

Mostafa Moini Obituary (2010). *The Oklahoman*. URL: https://obits.oklahoman.com/obituaries/oklahoman/obituary.aspx?pid=145211178.

Mouton, Yuan Horas (n.d.). *Increasing Anonymity in Bitcoin*. URL: https://download.wpsoftware.net/bitcoin/wizardry/horasyuanmouton-owas.pdf.

Murphy, Robert P. (2010). *Is Our Money Based on Debt?* Mises Institute. URL: https://mises.org/library/our-money-based-debt.

Nakamoto, Satoshi (Oct. 2008a). *Bitcoin P2P E-Cash Paper*. URL: https://satoshi.nakamotoinstitute.org/emails/cryptography/threads/1/.

— (Nov. 2008b). *Bitcoin P2P E-Cash Paper*. URL: https://satoshi.nakamotoinstitute.org/emails/cryptography/4/#selection-43.0-47.168.
— (2008c). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Satoshi Nakamoto Institute. URL: https://bitcoin.org/bitcoin.pdf.
— (2009a). *Bitcoin Open Source Implementation of P2P Currency. P2P Foundation*. URL: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.
— (Jan. 2009b). *Bitcoin v0.1 Released*. URL: https://satoshi.nakamotoinstitute.org/emails/cryptography/threads/2/.
— (Jan. 2009c). *Bitcoin v0.1 Released*. URL: https://satoshi.nakamotoinstitute.org/emails/cryptography/17/.
Nakamura, Yuji (Sept. 2017). "North Korea Hackers Step Up Bitcoin Attacks". In: *Bloomberg.com*. Accessed 24 August 2020. URL: https://www.bloomberg.com/news/articles/2017-09-11/north-korea-hackers-step-up-bitcoin-attacks-amid-rising-tensions.
Nelson, Danny (Dec. 2019). "Binance Blockade of Wasabi Wallet Could Point to a Crypto Crack-Up". In: *Coindesk*. URL: https://www.coindesk.com/binance-blockade-of-wasabi-wallet-could-point-to-a-crypto-crack-up.
Noether, Shen (2015). *Ring Confidential Transactions*. Tech. rep. Monero Research Labs. URL: https://eprint.iacr.org/2015/1098.pdf.
nopara73 (2017). *ZeroLink: The Bitcoin Fungibility Framework*. URL: https://github.com/nopara73/ZeroLink.
Obstfeld, Maurice, Jay C. Shambaugh, and Alan M. Taylor (2005). "The Trilemma in History: Tradeoffs among Exchange Rates, Monetary Policies, and Capital Mobility". In: *The Review of Economics and Statistics* 87.3, pp. 423–438. DOI: 10.1162/0034653054638300.
ONG Bitcoin Argentina (2020). *Quienes Somos*. Accessed 31 August 2020. URL: https://www.bitcoinargentina.org/quienes-somos/.
Orrell, David (2018). *Quantum Economics: The New Science of Money*. Icon Books Ltd. URL: https://libgen.rs/book/index.php?md5=1DBB6BA06C726CD7A75CF5E40B6F1CEE.
Orzi, Ricardo, Ricardo Borrello, et al. (2012). *La Moneda Social y Mercados Solidarios II: La Moneda Social Como Lazo Social*. 1st. Vol. 2. Editorial CICCUS. URL: https://www.academia.edu/3884388/Moneda_Social_y_mercados_Solidarios_II_la_moneda_social_como_lazo_social.

Orzi, Ricardo, Adela Plasencia, and Ricardo Borrello (2007). *Moneda Social y Mercados Solidarios I: Potencial Emancipador y Pedagógico de los Sistemas Monetarios Alternativos*. Vol. 2. Editorial CICCUS. URL: https://www.researchgate.net/publication/273137740_Moneda_social_y_mercados_solidarios_I_Potencial_emancipador_y_pedagogico_de_los_sistemas_monetarios_alternativos_2007.

Pastor, Javier (Apr. 15, 2020). *China Prepara su Criptomoneda Digital Oficial, Llamada DC/EP, y Cuatro de sus Bancos ya Están Probándola en Móviles*. Accessed 22 August 2020. URL: https://www.xataka.com/empresas-y-economia/china-prepara-su-criptomoneda-digital-oficial-llamada-dc-ep-cuatro-sus-bancos-estan-probandola-moviles.

Perfil (Sept. 2019). "Macri Vuelve al Cepo: Habrá que Pedir Autorización para Comprar Dólares". In: *Perfil*. URL: https://www.perfil.com/noticias/economia/macri-vuelve-al-cepo-habra-que-pedir-autorizacion-para-comprar-dolares.phtml.

Poelstra, Andrew (2016). *Mimblewimble*. Tech. rep. WP Software. URL: https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf.

Poon, Joseph and Thaddeus Dryja (2016). *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*. URL: https://lightning.network/lightning-network-paper.pdf.

Porter, Kim (2020). *Cyberthreat Trends: 15 Cybersecurity Threats for 2020*. URL: https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html.

Pratap, Jai (Dec. 24, 2019). *What Can You Buy with Bitcoin?* URL: https://coinnounce.com/what-can-you-buy-with-bitcoin/.

Presidencia de la Nación Argentina (2020). *Aislamiento Social Preventivo y Obligatorio*. Boletín Oficial de la República Argentina. URL: https://www.boletinoficial.gob.ar/detalleAviso/primera/227042/20200320.

Ratna, Tanvi (2020). "Iran Has a Bitcoin Strategy to Beat Trump". In: *Foreign Policy*. Accessed 24 August 2020. URL: https://foreignpolicy.com/2020/01/24/iran-bitcoin-strategy-cryptocurrency-blockchain-sanctions/.

Ravenna, Florencia (2019). *What the Residents of Barrio 31 Slum Taught Us about Bitcoin*. URL: https://blog.muun.com/what-the-residents-of-barrio-31-slum-taught-us-about-bitcoin.

Rebossio, Alejandro (2015). *Argentina Libera el Control de Capitals*. El País, 17 December 2015. URL: https://elpais.com/internacional/2015/12/16/argentina/1450304378%5C_455626.htm.

Reynoso, Carlos (2006). *Complejidad y Caos: Una Exploración Antropológica*. URL: https://www.academia.edu/26265561/Complejidad%5C_y_Caos_Una_Exploraci%C3%B3n_Antropol%C3%B3gica_Carlos_Reynoso.

— (2011). *Redes sociales y complejidad: Modelos Interdisciplinarios en la Gestión Sostenible de la Sociedad y la Culturan*. Complejidad Humana. URL: https://www.academia.edu/53341231/Redes_sociales_y_complejidad_Modelos_interdisciplinares_en_la_gesti%C3%B3n_sostenible_de_la_sociedad_y_la_cultura_2011_.

Rick, D. (2020). *Usuarios Retiran $200 Millones de Coinbase tras Acuerdo con el Gobierno de EE. UU.* BeInCrypto, 12 June 2020, accessed 24 August 2020. URL: https://es.beincrypto.com/usuarios-retiran-200-millones-dolares-coinbase-tras-acuerdo-gobierno-eeuu/.

Rodríguez, Víctor M. (2017). *Nace en la Argentina MonedaPar, Propuesta de Dinero Social*. Rebelión, 11 March 2017. URL: https://rebelion.org/nace-en-la-argentina-monedapar-propuesta-de-dinero-social/.

Rybarczyk, Rachel, Drew Armstrong, and Amanda Fabiano (2021). *On Bitcoin's Energy Consumption: A Quantitative Approach to a Subjective Question*. Galaxy Digital Mining 18.

Sasamans Society (n.d.). *Kwakwaka'wakw (Kwakiutl) copper*. URL: https://www.sasamans.ca/dzawadaenuxw-first-nation/.

Savage-Rumbaugh, E. Sue, Duane M. Rumbaugh, and Sally Boysen (1978). "Linguistically Mediated Tool Use and Exchange by Chimpanzees (Pan Troglodytes)". In: *Behavioral and Brain Sciences* 1.4, p. 539. DOI: 10.1017/s0140525x00076536.

Sceller, Quentin Le et al. (2018). *Introducción a Mimblewimble y Grin*. URL: https://github.com/mimblewimble/grin/blob/master/doc/intro%5C_ES.md.

Schargo, Carlos G. (2003). "Timing the Origin of New World Monkeys". In: *Molecular Biology and Evolution* 20.10, pp. 1620–1625. DOI: 10.1093/molbev/msg172.

Schurtz, Heinrich (1898). *Grundriss einer Entstehungsgeschichte des Geldes*. E. Felber. URL: https://archive.org/details/bub%5C_gb%5C_aJtAAAAAYAAJ/mode/2up.

Smialek, Jeanna and Peter Eavis (2020). *With $2.3 Trillion Injection, Fed's Plan Far Exceeds Its 2008 Rescue*. New York Times, 9 April 2020. URL: https://www.nytimes.com/2020/04/09/business/economy/fed-economic-rescue-coronavirus.html.

Smith, Adam (1977). *An Inquiry into the Nature and Causes of the Wealth of Nations*. University of Chicago Press. URL: https://libgen.rs/book/index.php?md5=82D82B24C8C2EFDACCE57357B85418DA.

Smith, Paul (2014). "Flowback or the End of Globalization". In: *IIM Kozhikode Society & Management Review* 3.1, pp. 1–9. DOI: 10.1177/2277975214535143.

Social Solidarity Economy Resource Website (n.d.). Heloisa Primavera. URL: https://ucc.socioeco.org/bdf_auteur-122_en.html.

Soulava from Trobriand (n.d.). https://pinterest.com/pin/145522631685932987/. Pinterest.

Stearns, Robert E. C. (1877). "Aboriginal Shell Money". In: *The American Naturalist* 11.6, pp. 344–350. DOI: 10.2307/2447731.

Szabo, Nick (1997). "Formalizing and Securing Relationships on Public Networks". In: *First Monday*. URL: https://firstmonday.org/ojs/index.php/fm/article/view/548/469.

— (2008). *Bit Gold*. http://unenumerated.blogspot.com/2005/12/bit-gold.html. *Unenumerated*.

Talk Alternatives (2020). *About Mutual Credit Systems, Cryptos & the FairCoop Community - with Guy James*. https://www.youtube.com/watch?v=RWlkOb_GhuU.

"Telecom: Un Ataque de Ransomware Afectó a sus Servicios; le Pidieron US$7,5 Millones de Rescate" (2020). In: *La Nación*. 19 July 2020. URL: https://www.lanacion.com.ar/tecnologia/reportan-ataque-ransomware-telecom-piden-us75-millones-nid2399977.

Tether (2016). *Tether: Fiat Currencies on the Bitcoin Blockchain*. https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf.

Thankful_for_today (2014). *[ANN][BMR] Bitmonero - a New Coin Based on CryptoNote Technology – LAUNCHED*. https://bitcointalk.org/index.php?topic=563821.0. Bitcoin Forum.

Thomsen, Christian Jürgensen (1836). "A Brief Overview of Monuments and Antiquities from the Nordic Past". In: *Guide to Northern Archaeology*. Royal Society of Northern Antiquaries.

Todd, Peter (2014). *Stealth Addresses*. https://sourceforge.net/p/bitcoin/mailman/message/31813471/. SourceForge.

Todd, Peter et al. (2020). *BIP-0065: OP_CHECKLOCKTIMEVERIFY*. https://github.com/bitcoin/bips. GitHub, accessed 17 August 2020.

Torpey, Kyle (2017). "Bitcoin Is Now Useless for Micropayments, But Solutions Are Coming". In: *Bitcoin Magazine*. 14 March 2017. URL: https://bitcoinmagazine.com/articles/bitcoin-now-useless-micropayments-solutions-are-coming1.

Tribal Art Finder (n.d.). Pinterest. URL: https://www.pinterest.com/pin/16184879884147121/.

Venkatakrishnan, Shaileshh Bojja, Giulia Fanti, and Pramod Viswanath (2017). *Dandelion: Redesigning the Bitcoin Network for Anonymity*. URL: https://arxiv.org/pdf/1701.04439.pdf.

Vigna, Paul (2018). "Pay Taxes With Bitcoin? Ohio Says Sure". In: *Wall Street Journal*. 26 November 2018. URL: https://www.wsj.com/articles/pay-taxes-with-bitcoin-ohio-says-sure-1543161720.

Walras, Léon (1874). *Éléments d'Économie Politique pure ou Théorie de la Richesse Sociale*. L. Corbaz & cie. URL: https://archive.org/details/lmentsdconomiep01walrgoog.

— (1965). *Elements of Pure Economics or The Theory of Social Wealth*. George Allen and Unwin ltd. URL: https://archive.org/details/elements-of-pure-economics_Leon-Walras/mode/2up.

Westergaard, Gregory C., Theodore Avery Evans, and Sue Howell (2007). "Token Mediated Tool Exchange between Tufted Capuchin Monkeys (Cebus Apella)". In: *Animal Cognition* 10.4, pp. 407–414. DOI: 10.1007/s10071-007-0072-9.

Westergaard, Gregory C., Chanya Liv, Tara J. Chavanne, et al. (1998). "Token-Mediated Tool-Use by a Tufted Capuchin Monkey (Cebus Apella)". In: *Animal Cognition* 1.2. DOI: 10.1007/s100710050014.

Westergaard, Gregory C., Chanya Liv, Andrea M. Rocca, et al. (2004). "Tufted Capuchins (Cebus Apella) Attribute Value to Foods and Tools during Voluntary Exchanges with Humans". In: *Animal Cognition* 7.1, pp. 19–24. DOI: 10.1007/s10071-003-0181-z.

Wicksell, Knut (1946). *Lectures on Political Economy. Vol. II: Money*. 2nd. Vol. 2. G. Routledge & Sons. URL: https://archive.org/details/in.ernet.dli.2015.73595/page/n8/mode/2up.

Wolfe, John Bascom (1936). *Effectiveness of Token Rewards for Chimpanzees*. Vol. 12. Comparative Psychology Monographs 5. The Johns Hopkins Press. URL: https://www.worldcat.org/title/effectiveness-of-token-rewards-for-chimpanzees/oclc/824092.

Worthpoint (n.d.). *Primitive Money Ndap Shell Coin Of Rossel Island Kejem Denomination*. URL: https://www.worthpoint.com/worthopedia/primitive-money-ndap-shell-coin-424120103.

Yukepo (n.d.). *Mokos from Alor*. URL: https://www.yukepo.com/hiburan/indonesiaku/moko-benda-purbakala-yang-dilestarikan-masyarakat-alor-ini-jadi-bukti-kalau-indonesia-keren/.

Cryptocurrencies, with more than ten years of existence, are no longer a phenomenon that could be called novel. However, it is still largely unexplored by the social sciences and humanities. Some work has been done in this sense, but it is more oriented towards dissemination than academic discussion. It is, then, a first objective of this book to introduce Bitcoin, cryptocurrencies and blockchains in the social sciences, from an anthropological and economic perspective, without neglecting their mathematical and technical foundations. Secondly, this work is a study of cryptocurrencies as one form of currency among others. However, in order to carry out such an undertaking, it was necessary to address the history, if not of money itself, then of studies about it. Money and currency are rather marginal objects of study in both anthropology and economics. Those who are familiar with the most important authors and schools in anthropology will notice the almost total absence of any mention of them in this study. That is why the entire first part is not devoted to cryptocurrencies but to currencies in general and to the theories that exist about them, both in economics and anthropology. This work is, therefore, a study of money and currencies in general, including cryptocurrencies.

ISBN 978-631-00-9715-2